NHS
Bradford District Care
NHS Foundation Trust

Records Management Policy

The 5 key messages the reader should note about this document are:

1. Good records management protects service users and staff and helps to provide consistent, high quality services
2. The Trust is committed to compliance with the laws and standards designed to protect information
3. All staff are accountable and responsible for the records they make and use
4. Audits and checks will be carried out across all services/sites to check compliance with this Policy and Procedural Guide
5. Training and advice is available – contact the Information Governance and Records Management team

This document has been approved and ratified. Circumstances may arise where staff become aware that changes in national policy or statutory or other guidance (e.g. National Institute for Health and Care Excellence (NICE) guidance and Employment Law) may affect the contents of this document. It is the duty of the staff member concerned to ensure that the document author is made aware of such changes so that the matter can be dealt with through the document review process.

NOTE: All approved and ratified policies and procedures remain extant until notification of an amended policy or procedure via Trust-wide notification, e.g. through the weekly e-Update publication or global e-mail and posting on the Intranet (Connect).

Procedural Document Title:	Records Management Policy.
Version:	11.1
Name and Title of Responsible Director/Senior Manager:	Tim Rycroft, Associate Director of Informatics/CIO/SIRO
Name and Title of Author	Gaynor Toczek, Information Governance and Records Manager/DPO
Title of Responsible Committee / Group (or Trust Board):	Information Governance Group.
Persons/Groups/Committees consulted:	All members of the Information Governance Group.
Service User, Patient and Carer consultation:	N/A
Procedural Document Compliance Checklist adhered to:	Yes
Target Audience:	All Staff
Approved by:	The Information Governance Group
Date Approved:	28th September 2018
Ratified by:	Executive Management Team
Date Ratified:	24/10/2017
Date Issued:	28th September 2018
Review Date:	Minor review 2018. Full review 2020
Frequency of Review:	Minor Review Annually, Major Review 3 yearly

Responsible for Dissemination:	Gaynor Toczek, Information Governance and Records Manager/DPO
Copies available from:	Connect on BDCFT Intranet.
Where is previous copy archived (if applicable)	Connect on BDCFT Intranet.
Amendment Summary:	Change of Director, Replaced DPA 1998 with DPA 2018, Added GDPR, Added the role of the DPO, Added new individual rights under GDPR, Removed all mentions of RiO, Changed the email guide post 365 accreditation, Added consent policy, Removed HR Solutions contact details, Added RCN Guide to giving statements

Amendment detail:

Amendment number	**Page**	**Subject**
1	2	Change of Director
2	All	Replaced DPA 1998 with DPA 2018,
3	13	Added new individual rights under GDPR
4	11	Added the role of the DPO,
5	All	Removed all mentions of RiO
6	52	Changed the email guide post 365 accreditation,
7	22	Added consent policy
8		Removed HR Solutions contact details
9	60	Added RCN Guide to giving statements

Contents

1 INTRODUCTION

Bradford District Care NHS Foundation Trust (BDCFT) is committed to compliance with the laws and standards designed to protect information through every phase of its existence, from creation through to destruction.

The key statutory requirements for compliance with records management principles are the Freedom of Information Act 2000, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). These together with the Records Management Code of Practice for Health and Social Care (2016) and the Information Security Management: NHS Code of Practice set the standards the Trust must achieve.

This policy outlines how the Trust will meet its legal obligations and NHS requirements in respect of records management and information security.

The appendices attached to this policy outline the procedures and provide guidance for all staff when working with records.

2 SCOPE

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

Records are a valuable resource because of the information they contain. High quality information underpins the delivery of high quality evidence based healthcare, and many other key service deliverables. Information has most value when it is accurate, up to date and accessible when it is needed.

All records produced by BDCFT will be managed to ensure that, from the moment a record is created until its ultimate disposal, the Trust can:

- control the quality and quantity of records created
- maintain the information in a manner that effectively serves its own needs and those of its stakeholders
- dispose of the record in accordance with Trust and Department of Health guidance

BDCFT is committed to the ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- better use of physical and electronic storage space
- better use of time
- improved control of valuable information resources
- compliance with legislation and standards
- reduced costs

The Trust also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated yet integrated corporate function.

The general principles of Records Management apply to all records created by BDCFT. The Trust uses different terms for the people that access its services, the term “service user” will be used throughout this policy to denote those who receive care and/or treatment within BDCFT. The term “staff” will be used to denote all people employed by the Trust whether on a permanent or temporary contract, an agency staff, volunteer or contractor.

This policy applies to all types and formats of records in BDCFT, including:

Function:

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

Format:

- Paper Records
- Photographs, slides, and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc
- E-mails
- Computerised/electronic records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to service users and staff.
- Leaflets and other similar promotional material created by BDCFT
- Policies and procedures together with other processes, such as records inventories, audit reports etc

3 RECORDS MANGEMENT POLICY AND PROCEDURES

3.1 Duties

3.1.1 The Chief Executive

The Chief Executive has the ultimate legal responsibility for ensuring appropriate mechanisms are in place to support Records Management within the Trust.

3.1.2 The Caldicott Guardian

The Caldicott Guardian has particular responsibility for acting as the conscience of the organisation and reflecting service user interests regarding the use of person identifiable Information. The Caldicott Guardian is responsible for ensuring person identifiable information is shared in an appropriate and secure manner. This role is currently performed by the Medical Director

3.1.3 The Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has an essential role in ensuring that identified information security risks are followed up and incidents managed. The role is supported by the Trust's Information Governance lead, Information Asset Owners and the Caldicott Guardian. This role is currently performed by the Trust Secretary.

3.1.4 Information Asset Owners (IAOs)

All information assets belonging to the Trust have been assigned to an Information Asset Owner.

All IAOs must:

Understand and address any risks to the information asset they 'own'.

Lead and foster a culture that values, protects and uses information for the success of the organisation and benefits its service users.

Know what information their assets hold, what enters it, leaves it and why.

Know who has access to their assets and why, and ensures their use is monitored and compliant with policy.

Ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of the Trust.

Be accountable to the SIRO to provide assurance on the security and use of their information assets.

Complete the Information Risk Management for SIROs and IAOs e-learning module annually.

3.1.5 The Trust Board

The Board is responsible for supporting and endorsing policy decisions made by its delegated authorities

3.1.6 Information Governance (IG) Group

This group acts as the Information Governance steering group and is responsible for ensuring that the records management strategy and policy are implemented. It is also responsible for ensuring records management systems and processes are developed, co-ordinated and managed. It reports to the Informatics Board.

3.1.7 Deputy Directors and Heads of Service

Deputy Directors and Heads of Service are responsible for local records management. Heads of Departments/ Professional leads within the organisation have overall responsibility for the management of records generated by their activities, i.e. ensuring that records controlled within their unit are managed in a way which meets the aims of the organisation's Records Management policies. They are also responsible for ensuring that the actions resulting from an audit are implemented in their area.

3.1.8 Information Governance and Records Manager/Data Protection Officer (DPO)

The Information Governance and Records Manager is the Information Governance Lead and Data Protection Officer and is responsible for the overall development and maintenance of records management practices throughout the organisation, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of service user information. These duties include helping to embed processes, arranging audit of the process and providing training.

3.1.9 All Workers

Staff who create, receive and use records for the Trust 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 policy and with any guidance subsequently produced. In addition, all staff have a duty to make themselves aware of this Policy, and the associated Procedure Guide.

All staff are accountable and responsible for the records they make whether or not they hold a professional qualification. Professionals are personally accountable for their practice and, in the exercise of their professional accountability, must act in such a manner as to promote and safeguard the interests and wellbeing of service users; and ensure that no action or omission on their part, or within their sphere of responsibility, is detrimental to the interests, condition, or safety of service users. This accountability extends to the making and keeping of service user records, which is an integral part of care.

3.1.10 Individual Responsibility

Under the Public Records Act 1958 employees are responsible for any records that they create or use in the course of their duties. Therefore, any records created or received by an employee of the NHS are public records and may be subject to both legal and professional obligations

3.1.11 Contractors and support organisations

Service Level Agreements and contracts must include responsibilities for information governance and records management as appropriate

3.1.12 Breaches to this Policy

If there is an incident or breach of this Record Management policy staff should follow the Incident Management policy and related procedures by completing an IR-e on Connect.

If a records issue is deemed to be a Serious Incident (SI) staff should follow the Management of Serious Incident policy and procedures: Incident Management Policy and procedures. Any identified risks associated with Records will be placed on the appropriate Service or Directorate Risk Register(s), which, in turn, feeds into the Trust Risk Register process as part of the Trust's Risk Management Strategy.

The Records Management Information Lifecycle

This describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest.

3.2 The information lifecycle defines 5 distinct phases:

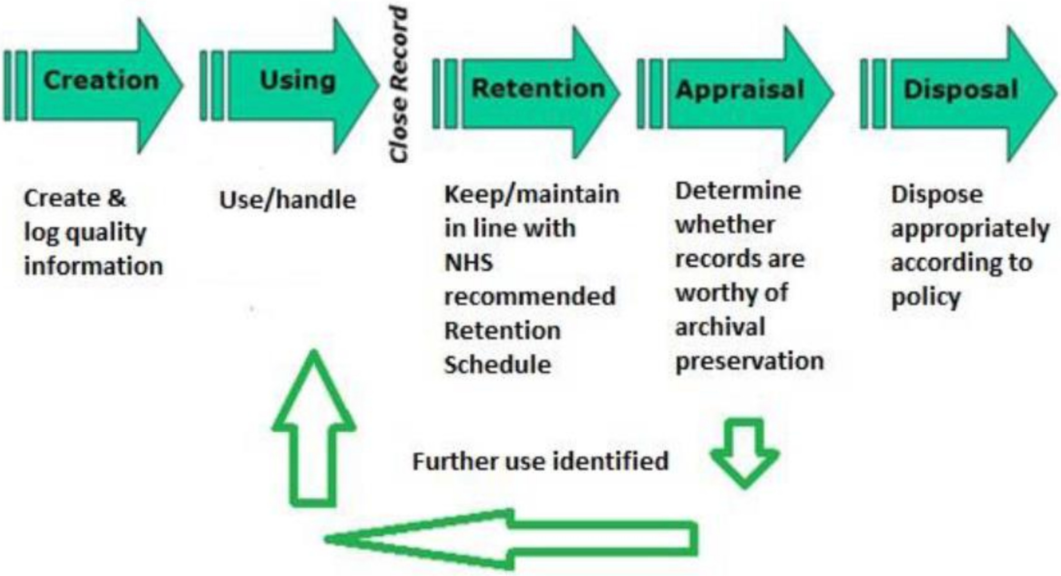
1. Creation

2. Use

3. Retention

4. Appraisal

5. Disposal


Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log quality information
Use/handle
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of archival preservation
Dispose appropriately according to policy
Further use identified

The Records Management procedures underpinning this document cover the details for each of these phases and the Trust's staffs' obligations under this policy. This policy covers the obligations of all organisations employed by the Trust, all organisations contracted to the Trust and any organisation, or third party that shares Person Identifiable Information with the Trust

3.3 Creation

This part of the life cycle is begins when we make an entry into a database or start a new electronic document. A record can be created by internal employees or received from an external source. New records are created daily. All records created by staff within the Trust are subject to this policy.

A record must be created for all new staff and service users.

Advice and guidance for creating a new record can be found in **Appendix G.**

Advice and guidance for corporate records (non-service user or staff) refer to the **Development and Management of Procedural Documents policy**.

3.4 Use

This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other NHS Trust

Further information About Records Security: Work Base, Home Working, Agile Working may be found in Appendix J

3.4.1 Record Access and Disclosure

There is a range of statutory duties that give individuals the right of access to information created or held by the Trust such as a Subject Access Request under the Data Protection Act 2018, General Data Protection Regulation or a Freedom of Information Act request.

The Data Protection Act 2018 allows individuals to find out what personal data is held about them, to view them and to request copies of the same. In addition individuals have the right:

- to have inaccuracies corrected,
- to have information erased,
- to prevent direct marketing,
- to prevent automated decision-making and profiling, and
- data portability.

The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities.

Statutory duties may limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly statutory duties that require or permit disclosure.

Only the IG&RM team together with the Caldicott Guardian have the authority to disclose records. The IG&RM team make a record of any copies of records they have disclosed, and to whom.

Advice and guidance for access to personal records and disclosure can be found in the **Confidentiality and Data Protection Policy** and related procedures.

Advice and guidance for access to corporate records and documents can be found in the **Freedom of Information policy** and procedures.

Further guidance on maintaining records may be found in **Appendix F.**

Further information on the use of records may be found i**n Appendix G**

3.5 Retention

All records created by the NHS must be retained for a minimum period of time, including emails and diaries. BDCFT has adopted the national guidance from the Records Management Code of Practice for Health and Social Care 2016.

Advice and guidance for record retention can be found in **Appendix E.**

3.5.1 Maintenance

Maintenance is when records are not used on a day to day basis and are stored in a Records Management system or store (such as a database or record store). Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. Maintenance includes filing, tracking, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be permanently removed from a Records Management system/store.

Further guidance on maintaining records may be found in **Appendix F.**

3.5.2 Storage

Paper: to establish the authenticity of paper records and to meet the Care Records Guarantee (that the service user can see who has accessed their records), paper records will be held according to a standard that allows access to be audited.

The Trust will actively manage records which are stored offsite. The Trust will ensure that it maintains a full inventory of what is held offsite, that retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers.

Digital: digital information will be stored in such a way that throughout the lifecycle it can be recovered in an accessible format in addition to providing information about those who have accessed the record, as required by the Care Records Guarantees.

3.6 Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. No record or series can be automatically destroyed or deleted. The Information Governance Group is responsible for authorising the deletion or destruction of Trust records.

There will be one of three outcomes from appraisal:

- Destroy / delete
- To keep for a longer period

- To transfer to a place of deposit appointed under the Public Records Act 1958.

The retention schedule included in this policy lists those records which should or may be selected for transfer to a place of deposit. There are also a number of other records which may be of interest to a local place of deposit. Appraisal may also result in a record being retained for longer.

If as a result of appraisal, a decision is made to destroy a record there must be evidence of the decision.

Records transferred to a place of deposit, such as unpublished board papers, may continue to be subject to FOIA exemptions on public access following transfer.

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. Decisions can then be applied to an entire class of records rather than reviewing each record in turn.

3.7 Disposal

Disposal is when a record is less frequently accessed, has no more value to the Trust or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value will be kept and sent to the National Archives, where it will be kept for the future of the organisation and may never be destroyed. This is the final phase of a records lifecycle.
Records should only be destroyed as per NHS England's Policy. It can be a personal criminal offence to destroy requested information under either the Data Protection Act or the Freedom of Information Act. Therefore, the Trust needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures.

Further information on record disposal may be found in **Appendix H**

4 DEFINITIONS

4.1 Access

The availability of, or permission to view records.

4.2 Archiving

The storing of files, records and other data for reference.

4.3 Breach of Confidentiality

The unauthorised disclosure of personal confidential information.

4.4 Caldicott Guardian

The person within an NHS organisation who is responsible for protecting service user data.

4.5 Confidential Information

Privileged communication shared with only a few people for furthering certain purposes, such as with a doctor for treatment. Person identifiable information is held under a duty of confidentiality. This includes information about their condition, and where they are being treated. Certain information about staff, contracts and tenders may also be confidential.

4.6 Corporate Records

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

4.7 Current Records

Records necessary for conducting the current and on-going business of the Trust

4.8 Destruction

The process of eliminating or deleting records beyond any possible reconstruction

4.9 Disposal

The destruction of or transfer of custody of records (including the transfer of selected records to an archive institution) following appraisal and review decisions.

4.10 Electronic Records

Records where the information is recorded in a form that is suitable for retrieval, processing and communication by digital technology

4.11 Paper Records

In the form of files, volumes, folders, bundles, maps, plans, diaries etc. (this list is not exhaustive)

4.12 Person Identifiable Information (PID)

Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Key identifiable information includes:

- Service user's name, address, full post code, date of birth
- Pictures, photographs, videos, audio-tapes or other images of service users
- NHS number and local service user identifiable codes
- Anything else that may be used to identify a service user directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

4.13 Public Record

Records defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives.

4.14 Record

Anything which contains information created or gathered as a result of any aspect of the work of Trust employees.

4.15 Records Management

Responsible for the efficient and systematic control of creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

4.16 Scanning

The process of transferring one document, or a series of documents, into a form that is suitable for retrieval, processing and communication by digital technology

4.17 Records Life Cycle

Describes the life of a record: from its creation or receipt; throughout its time in active use; into a period of retention; and finally either confidential disposal or archival preservation.

5 EQUALITY IMPACT ASSESSMENT

The Trust has no intent to discriminate and endeavours to develop and implement policies that meet the diverse needs of our workforce and the people we serve, ensuring that none are placed at a disadvantage over others. Our philosophy and commitment to care goes above and beyond our legal duty to enable us to provide high-quality services. Our Equality Analysis and equality monitoring is a core service improvement tool which enables the organisation to address the needs of disadvantaged groups. The aim of Equality analysis is to remove or minimise disadvantages suffered by people because of their protected characteristics.

An impact assessment has been undertaken to consider the need and assess the impact of this Procedural Document and is evidenced at Appendix A.

6 TRAINING NEEDS ANALYSIS

The Trust is committed to high quality targeted training and effective communication to support this procedural document. The Trust recognises that training capacity can fluctuate and will depend on resources available. As such, based on an assessment of capacity and risk, the training needs analysis will identify the high priority groups for training. The objective is to implement this procedural document and meet the training needs of these groups over the time frequency stated. The focus of Trust monitoring will be on this group over the agreed period or lifetime of the procedural document.

7 MONITORING COMPLIANCE AND EFFECTIVENESS

Criteria	Evidence identified to indicate compliance with policy	Method of monitoring, i.e. how/where will this be gathered?	Frequency of monitoring	Lead responsible for monitoring
Duties	For incident management, which includes Records incidents: Minutes of Trust Board, Audit Committee, QSC, quality and safety governance groups. Completed Incident Forms Investigation Reports Internal Audit Reports Annual reports Quarterly reports Annual incident management reports Monthly incident reports to services Incident report schedule maintained in risk management and drive	Safeguard System Minutes/discussions at meetings Internal audit Reports Annual report	Annually	Safety, Risk & Resilience Manager

Criteria	Evidence identified to indicate compliance with policy	Method of monitoring, i.e. how/where will this be gathered?	Frequency of monitoring	Lead responsible for monitoring
Duties	SIRO and Caldicott Guardian receive IG and Records incident reports Information Governance Group receives quarterly updates for IG and records incidents and performance Reports to Information Governance Group	Monitored through the Incident Management System Incident reports, Audits of sites for record activities, S1 audits and external audit reports	Monthly Every 8 weeks	IG&RM Coordinator IG&R Manager
Legal Obligations that apply to Records	SIRO, Caldicott, and IG Group receive quarterly reports on compliance with requests for information under the Data protection and Freedom of Information Act	All requests are logged and monitored via the Safeguard Database	Quarterly	IG&R Manager
How a new record is created	Record audit schedule, audit reports to managers and improvement plans. Results are reported to IG Group by exception.	The IG&RM team audit the creation of records by site and teams throughout the year	Every 8 weeks	IG&R Manager

Criteria	Evidence identified to indicate compliance with policy	Method of monitoring, i.e. how/where will this be gathered?	Frequency of monitoring	Lead responsible for monitoring
How health records are tracked when in current use	Record audit schedule, audit reports to managers and improvement plans. Results are reported to IG Group by exception.	The IG&RM team audit the tracking of records by site and teams throughout the year	Every 8 weeks	IG&R Manager
How health records are retrieved from storage	Record audit schedule, audit reports to managers and improvement plans. Results are reported to IG Group by exception	The IG&RM team audit the retrieval of records by site and teams throughout the year	Every 8 weeks	IG&R Manager
Process for retention, disposal and destruction of records	Record audit schedule, audit reports to managers and improvement plans. Results are reported to IG Group by exception.	The IG&RM team audit the tracking of records by site and teams throughout the year	Every 8 weeks	IG&R Manager
a) basic recordkeeping standards, which must be used by all staff		Data collected by the different leads for audit projects and activities	Annually	IG&R Manager
b) how the organisation trains staff, in line with the training needs analysis	Training records for induction, IG, Records Management, Induction and Doctor's induction	Training records are inputted to the ESR system	6 monthly	IG&R Manager

8 REFERENCES TO EXTERNAL DOCUMENTS

- Access to Health Records Act 1990
- Code of practice on confidential information
- Confidentiality NHS Code of Practice
- Data Protection Act 2018
- General Data Protection Regulation
- Freedom of Information Act 2000
- Guide to Confidentiality in Health and Social Care
- Information Security management NHS code of practice
- NHS Information Governance: Guidance on Legal and Professional Obligations
- Public Records Act 1958
- Records Management Code of Practice for Health and Social Care 2016 – Information Governance Alliance (IGA)
- Regulation of Investigatory Powers Act 2000

9 ASSOCIATED INTERNAL DOCUMENTATION

In respect of this policy, specific related Procedural Documents / Trust documents are:

- Incident Management Policy
- Management of Serious Incident policy and procedure
- Invited Guests Access Policy and Procedure
- Information Governance Policy and procedures
- Freedom of Information Act Policy and Procedures
- Development and Management of Procedural Documents Policy
- Data Protection Act Policy and procedures
- Information Security Policy and procedures
- Clinical Information Systems Policy
- Consent policy
- Data Quality Guidance Document
- SystmOne Procedures
- R4 Procedures
- PCMIS Procedures
- Everything Agile on the desktop
- Best Practice Guidance for Information Asset Owners and Information Asset Administrators

10 APPENDIX A: EQUALITY IMPACT ASSESSMENT (EQIA)

Area	Response
Policy/Procedure	Records Management policy
Manager	Information Governance and Records Manager
Directorate	Medical
Date	07/08/2017
Review date	August 2018
Purpose of Policy	To ensure all Trust Records are treated in accordance with legislation and NHS codes of practice
Associated frameworks e.g. national targets NSF's	CQC and Information Governance Toolkit
Who does it affect	All staff and service users
Consultation process carried out	Information Governance Group members
QA Approved by	IG Group

Equality protected characteristic	Impact Positive	Impact Negative	Rationale for response
Age	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Disability	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Gender Reassignment	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Race	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Religion or Belief	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Pregnancy &	√	None	There is currently no information that indicates

Equality protected characteristic	Impact Positive	Impact Negative	Rationale for response
Maternity			that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Sex	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern
Sexual Orientation	√	None	There is currently no information that indicates that this document will disadvantage or have a negative impact on this group if implemented and operated in a manner that is laid out within this document. We have had no feedback of any concern

Equality Analysis SIGN – OFF		
Have any adverse impacts been identified on any equality groups which are both highly significant and illegal?		No
Are you satisfied that the conclusions of the EqIA Screening are accurate? The Trust will publish a summary of the impact analysis carried out to meet the duty and make this available to the public on the Trust Internet site.		Yes
Completed by Manager	Information Governance and Records Manager	
Q A approved	IG Group	
Director approved	Medical Director	

PROCEDURAL DOCUMENT COMPLIANCE CHECKLIST

The Procedural Document Compliance Checklist is available to the Author to ensure a uniform approach to its development and management and should be utilised as a source of assurance by them and the Director/ Senior Manager responsible for it to ensure that all requirements are met.

The Procedural Document Compliance Checklist will not be included in the final version of the Procedural Document and should be removed from the final version of it and filed separately by the Author.

The Author must indicate in the Production and Review Details on page 2 of the Procedural Document that they have produced the Procedural Document in a manner that is compliant with the Procedural Document Compliance Checklist. Failure to do this will mean that the Procedural Document cannot proceed to approval and ratification. (This requirement was set by the Non-Clinical Policy Ratification Group on 30/11/2015).

Insert title of document being reviewed		**Yes/No/ Unsure**	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?	y	
	Is it clear whether the document is a policy or procedure?	y	
2.	**Rationale**		
	Are reasons for development of the procedural document stated, e.g. in the Introduction or Scope sections?	y	
3.	**Development Process**		
	Is the method described in brief e.g. in the Introduction or Scope sections?	y	
	Are people involved in the development identified, e.g. in the Production and Review Details (page 2)?	y	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	y	
	Is there evidence of consultation with stakeholders, service users, patients or carers, e.g. in the Production and Review Details (page 2)?	y	
	Have the requirements of the following been taken into account where applicable: Mental Health Act Mental Capacity Act Care Programme Approach (CPA) Guidance	y	
4.	**Content**		
	Is the objective of the document clear, e.g. in the Scope section?	y	
	Is the target population clear and	y	

Insert title of document being reviewed		**Yes/No/ Unsure**	**Comments**
	unambiguous, e.g. in the Scope section?		
	Are the intended outcomes described, e.g. in the Core Content section?	y	
	Are the statements clear and unambiguous?	y	
	Are any amendments compared to a previous version of the document summarised or where appropriate listed in more detail, e.g. in the Production and Review Details (page 2)?	y	
	The Trust is transitioning services to agile working: please consider and include implications for agile workers and the management of agile within all policies and procedures.	y	
	Accessible Information Standard. All organisations that provide NHS or adult social care are legally required to meet the standard law (Section 250 of the Health and Social Care Act 2012) and to ensure that people who have a disability, impairment or sensory loss are asked if they have any accessible information needs and if they do that these needs are met. This might include making sure that people get information in different formats if they need it, for example in large print, braille, easy read or via email or that people get support with communication that they need, for example support from a British Sign Language (BSL) interpreter, deafblind manual interpreter or advocate. Under the Standard organisations must do the following five things. So please consider when writing your policy and any associated procedures how you will: 1. Ask people if they have any information or communication needs and how these needs might be met. 2. Record those needs clearly and in a set way in the appropriate clinical system. 3. Highlight or flag the person’s file or notes so it is clear that they have information or communication needs and how to meet those needs. 4. Share information about people’s information and communication needs with other providers of NHS and adult	y	

	Insert title of document being reviewed	Yes/No/ Unsure	Comments
	social care, when they have consent or permission to do so. 5. Take steps to ensure that people receive information which they can access and understand, and receive communication support if they need it. For more information and support with the Accessible Information Standard contact Fiona Sherburn, Deputy Director of HR & Workforce Development.		
	Information Governance Insert something here about what the author of the procedure should consider in terms of information Governance and sharing information outside BDCFT plus a contact in the Information Governance Team for support. For more information about Information Governance contact: Gaynor Toczek, Information Governance and Records Manager/DPO.	y	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly, e.g. in the References to External Documents, Associated Internal Documentation sections and Appendices?	y	
	Are key references cited?	y	
	Are the references cited in full?	y	
	Are supporting documents referenced?	y	
6.	**Approval and Ratification**		
	Does the document identify which committee/group will approve it, e.g. in the Production and Review Details (page 2)?	y	
	If appropriate have the joint Human Resources/Staff Side Committee (or equivalent) approved the document, e.g. in the Production and Review Details (page 2)?	y	
	Does the document identify which committee/group will ratify it, e.g. in the Production and Review Details (page 2)?	y	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done, e.g. in the Production and Review Details (page 2)?	y	

Insert title of document being reviewed		**Yes/No/ Unsure**	**Comments**
	Does the plan include the necessary training/support to ensure compliance, e.g. in the Training Needs Analysis section?	y	
8.	**Document Control**		
	Does the document identify where it will be held, e.g. in the Production and Review Details (page 2)?	y	
	Have archiving arrangements for superseded documents been addressed, e.g. in the Production and Review Details (page 2)?	y	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable criteria, standards or KPIs to support the monitoring of compliance with and effectiveness of the document, e.g. in the Monitoring Compliance and Effectiveness section?	y	
	Is there a plan to review or audit compliance with the document e.g. in the Monitoring Compliance and Effectiveness section?	y	
10.	**Review Date**		
	Is the review date identified, e.g. in the Production and Review Details (page 2)?	y	
	Is the frequency of review identified? If so is it acceptable, e.g. in the Production and Review Details (page 2)?	y	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document, e.g. in the Production and Review Details (page 2)?	y	

Author Approval			
The Author should complete, sign and date this Procedural Document Compliance Checklist then share it with the Responsible Director/Senior Manager.			
Author	Gaynor Toczek	Date	07/08/2017
Signature			
Responsible Director/Senior Manager			
The Responsible Director/Senior Manager should complete, sign and date this then share it with the Responsible Director/Senior Manager. If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name		Date	
Signature			

11 APPENDIX C: TRAINING

11.1 Training Plan

The Trust is committed to high quality targeted training and effective communication to support this policy. The Trust recognises that training capacity can fluctuate and will depend on resources available. As such, based upon an assessment of capacity and risk, the training needs analysis will identify the high priority groups for training.

The objective of the training to implement this policy is to meet training to this group of staff over the time and frequency stated.

Issues relating to capacity to meet training needs for the high priority group will be escalated by the policy lead to the relevant Director for action to mitigate the risk and inclusion on the appropriate risk register.

Induction

All staff (including agency and locum staff) will be made aware of the Records Management Policy and the procedures to be followed via the induction programme.

E-learning

Further training is available via ESR
It is a mandatory requirement for all staff to complete the Data Security Awareness - Level 1 e-learning module annually.

Further training will be made available via
workshops

Bespoke Workshops may be arranged by contacting the Information Governance and Records Management team IG.department@bdct.nhs.uk

Communications

All new guidance and updated guidance will be circulated to all staff via the E-Comms Service and will be stored on the IG&R pages on Connect.

12 APPENDIX D: CREATING A RECORD

The Trust uses electronic record keeping for most clinical areas and staff should not be creating paper Single Patient Records (SPRs) as standard.*

Where services are using electronic databases such as SystmOne, PCMIS or R4 these systems should be the complete current service user record (except for old archived volumes).

Where services have not yet got access to electronic records for their record keeping they will have **no choice** other than to create paper records.

* It is recommended that the only time those with access to electronic records should be creating paper records are:

1. When they have been asked by the clinical systems team to invoke the Business Continuity Plan: that is, if it is known the system is going to be down for a period of time, or if the system or network crashes.

2. When the electronic record is not available to you as a clinician. Summary information may be printed off and destroyed once the electronic system has been updated (for example, summary information is printed from SystmOne to enable a home visit, this paper record is updated at the time of the visit. Any additions to the notes are then entered onto SystmOne at the earliest point, and the paper record destroyed).

For those services using an electronic system (for example SystmOne, PCMIS and R4 please refer to the guidance provided by the System Management team or individual system supplier.

The Trust maintains an Employee Staff Record on the ESR database. A record must be created for all new staff. Please refer to the guidance provided by the HR Service, this can be found on CONNECT.

Advice and guidance for corporate records (non-service user or staff) refer to the **Development and Management of Procedural Documents policy**.

13 APPENDIX E: RECORD RETENTION – HEALTH RECORDS

For service users who have recently been discharged, but who may be re-referred, paper records can be stored locally for up to 1 year. After a relevant period of no further activity the file can be sent to the Trust's Archive Facility. Please see appendix F for further information.

All type of Records created by the NHS **must** be retained for a minimum period of time. BDCFT has adopted the national guidance from the ***Records Management Code of Practice for Health and Social Care 2016.***

Below is a list of the main Records types created by BDCFT, each by their recommended or statutory retention period.

Important Note:

The Independent Inquiry into Child Sexual Abuse (IICSA) previously chaired by Hon. Dame Lowell Goddard and now chaired by Prof. Alexis Jay OBE has requested that large parts of the health and social care sector do not destroy any records that are, or may fall into, the remit of the inquiry. Investigations will take into account a huge range of records which may include, but are not limited to, adoption records, safeguarding records, incident reports, complaints and enquiries.

Broad descriptor	Record Type	Retention Start	Retention period	Action at end of retention period	Notes
Care Records with standard retention periods	Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with standard retention periods	Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	
Care Records with standard retention periods	Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Care Records with standard retention periods	Electronic Patient Records System	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.

Care Records with standard retention periods	General Dental Services records	Discharge or patient last seen	10 Years	Review and if no longer needed destroy	
Care Records with standard retention periods	GP Patient records	Death of Patient	10 years after death see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: 1. Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated 2. Where a patient is known to have emigrated, records may be reviewed and destroyed after 10 years 3. If the patient comes back within the 100 years, the retention reverts to 10 years after death.
Care Records with standard retention periods	Mental Health records	Discharge or patient last seen	20 years or 8 years after the patient has died	Review and if no longer needed destroy	Covers records made where the person has been cared for under the Mental Health Act 1983 as amended by the Mental Health Act 2007. This includes psychology records. Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be ongoing. Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge. All must be reviewed prior to destruction taking into account any serious incident retentions.
Care Records with standard retention periods	Obstetric records, maternity records and antenatal and post natal records	Discharge or patient last seen	25 years	Review and if no longer needed destroy	For the purposes of record keeping these records are to be considered as much a record of the child as that of the mother.

Care Records with Non-Standard Retention Periods	Cancer/Oncology - the oncology records of any patient	Diagnosis of Cancer	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main patient file the entire file must be retained. Retention is applicable to primary acute patient record of the cancer diagnosis and treatment only. If this is part of a wider patient record then the entire record may be retained. Any oncology records must be reviewed prior to destruction taking into account any potential long term research value which may require consent or anonymisation of the record.
Care Records with Non-Standard Retention Periods	Contraception, sexual health, Family Planning and Genito-Urinary Medicine (GUM)	Discharge or patient last seen	8 or 10 years (see Notes)	Review and if no longer needed destroy	Basic retention requirement is 8 years unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. If this is a record of a child, treat as a child record as above.
Care Records with Non-Standard Retention Periods	HFEA records of treatment provided in licenced treatment centres		3, 10, 30, or 50 years	Review and if no longer needed destroy	Retention periods are set out in the HFEA guidance at:http://www.hfea.gov.uk/docs/General_directions_0012.pdf
Care Records with Non-Standard Retention Periods	Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.
Care Records with Non-Standard Retention Periods	Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care.The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.

Pharmacy	Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guidance can be found at the link (subscription required) http://www.rpharms.com/support/mep.asp#new Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review.NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see:http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/
Pharmacy	Pharmacy prescription records *see also Controlled Drugs*	Discharge or patient last seen	2 Years	Review and if no longer needed destroy	See also 'Controlled Drugs'. There will also be an entry in the patient record and a record held by the NHS Business Services Authority. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/

Pathology	Pathology Reports/Information about Specimens and samples	Specimen or sample is destroyed	See Notes	Review and consider transfer to a Place of Deposit	This Code is concerned with the information about a specimen or sample. The length of storage of the clinical material will drive the length of time the information about it is to be kept. For more details please see: https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition Retention of samples for clinical purposes can be for as long as there is a clinical need to hold the specimen or sample. Reports should be stored on the patient file. It is common for pathologists to hold duplicate reports. For clinical purposes this is 8 years after the patient is discharged for an adult or until a child's 25th birthday whichever is the longer. . After 20 years for adult records there must be an appraisal as to the historical importance of the information and a decision made as to whether they should be destroyed of kept for archival value.
Event & Transaction Records	Blood bank register	Creation	30 Years minimum	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	Clinical Audit	Creation	5 years	Review and if no longer needed destroy	
Event & Transaction Records	Chaplaincy records	Creation	2 years	Review and consider transfer to a Place of Deposit	See also Corporate Retention
Event & Transaction Records	Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.

Event & Transaction Records	Clinical Protocols	Creation	25 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (see Corporate Records).
Event & Transaction Records	Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf
Event & Transaction Records	Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.
Event & Transaction Records	Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Event & Transaction Records	General Ophthalmic Services patient records related to NHS financial transactions	Discharge or patient last seen	6 Years	Review and if no longer needed destroy	
Event & Transaction Records	GP temporary resident forms	After treatment	2 years	Review and if no longer needed destroy	Assumes a copy sent to responsible GP for inclusion in the primary care record
Event & Transaction Records	Inspection of equipment records	Decommissioning of equipment	11 Years	Review and if no longer needed destroy	
Event & Transaction Records	Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	

Event & Transaction Records	Operating theatre records	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	If transferred to a place of deposit the duty of confidence continues to apply and can only be used for research if the patient has consented or the record is anonymised.
Event & Transaction Records	Patient Property Books	End of the year to which they relate	2 years	Review and if no longer needed destroy	
Event & Transaction Records	Referrals not accepted	Date of rejection.	2 years as an ephemeral record	Review and if no longer needed destroy	The rejected referral to the service should also be kept on the originating service file.
Event & Transaction Records	Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	
Event & Transaction Records	Screening, including cervical screening, information where no cancer/illness detected is detected	Creation	10 years	Review and if no longer needed destroy	Where cancer is detected see 2 Cancer / Oncology. For child screening treat as a child health record and retain until 25th birthday or 10 years after the child has been screened whichever is the longer.
Event & Transaction Records	Smoking cessation	Closure of 12 week quit period	2 years	Review and if no longer needed destroy	
Event & Transaction Records	Transplantation Records	Creation	30 Years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.hta.gov.uk/codes-practice
Event & Transaction Records	Ward handover sheet	Date of handover	2 years	Review and if no longer needed destroy	This retention relates to the ward. The individual sheets held by staff must be destroyed confidentially at the end of the shift.
Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 Years	Review and if no longer needed destroy	The period of time cited by the NHS Litigation Authority is 3 years

Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	Recorded conversation which forms part of the health record	Creation	Store as a health record	Review and if no longer needed destroy	It is advisable to transfer any relevant information into the main record through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record the recording must be considered as part of the record and be retained accordingly.
Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).	The telephony systems record(not recorded conversations)	Creation	1 year	Review and if no longer needed destroy	This is the absolute minimum specified to meet the NHS contractual requirement.
Births, Deaths & Adoption Records	Birth Notification to Child Health	Receipt by Child health department	25 years	Review and if no longer needed destroy	Treat as a part of the child's health record if not already stored within health record such as the health visiting record.
Births, Deaths & Adoption Records	Birth Registers	Creation	2 years	Review and actively consider transfer to a Place of Deposit	Where registers of all the births that have taken place in a particular hospital/birth centre exist, these will have archival value and should be retained for 25 years and offered to a Place of Deposit at the end of this retention period. Information is also held in the NHS Number for Babies (NN4B) electronic system and by the Office for National Statistics. Other information about a birth must be recorded in the care record.
Births, Deaths & Adoption Records	Body Release Forms	Creation	2 years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	Death - cause of death certificate counterfoil	Creation	2 years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	Death register information sent to General Registry Office on monthly basis	Creation	2 years	Review and consider transfer to a Place of Deposit	A full dataset is available from the Office for National Statistics.

Births, Deaths & Adoption Records	Local Authority Adoption Record (normally held by the Local Authority children's services)	Creation	100 years from the date of the adoption order	Review and consider transfer to a Place of Deposit	The primary record of the adoption process is held by the local authority children's service responsible for the adoption service
Births, Deaths & Adoption Records	Mortuary Records of deceased	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	Mortuary register	Creation	10 Years	Review and consider transfer to a Place of Deposit	
Births, Deaths & Adoption Records	NHS Medicals for Adoption Records	Creation	8 years or 25th birthday	Review and consider transfer to a Place of Deposit	The health reports will feed into the primary record held by Local Authority Children's services. This means that the adoption records held in the NHS relate to reports that are already kept in another file which is kept for 100 years by the appropriate agency and local authority.
Births, Deaths & Adoption Records	Post Mortem Records	Creation	10 years	Review and if no longer needed destroy	The primary post mortem file will be maintained by the coroner. The coroner will retain the post mortem file including the report. Local records of post mortem will not need to be kept for the same extended time.
Clinical Trials & Research	Advanced Medical Therapy Research Master File	Closure of research	30 years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials
Clinical Trials & Research	Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014	Closure of trial	25 years	Review and consider transfer to a Place of Deposit	For details see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG

Clinical Trials & Research	European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	Closure of trial	15 years	Review and consider transfer to a Place of Deposit	http://ec.europa.eu/health/files/eudralex/vol-2/a/vol2a_chap1_2013-06_en.pdf
Clinical Trials & Research	Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf
Clinical Trials & Research	Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to a Place of Deposit	For details please see:http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach.
Clinical Trials & Research	Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years	Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a place of deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/
Corporate Governance	Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	

Corporate Governance	Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Corporate Governance	Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Corporate Governance	Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings
Corporate Governance	Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument they must either be transferred to a place of deposit as a public record or destroyed 20 years after the record has been closed.
Corporate Governance	Incidents (serious)	Date of Incident	20 Years	Review and consider transfer to a Place of Deposit	
Corporate Governance	Incidents (not serious)	Date of Incident	10 Years	Review and if no longer needed destroy	
Corporate Governance	Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	

Corporate Governance	Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	
Corporate Governance	Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	
Communications	Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Communications	Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Communications	Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Communications	Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Communications	Website	Creation	6 years	Review and consider transfer to a Place of Deposit	
Staff Records & Occupational Health	Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Staff Records & Occupational Health	Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	

Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Records & Occupational Health	Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see page 36 for an example of a Staff Record Summary used by an organisation.
Staff Records & Occupational Health	Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer2 Statutory and mandatory training records - to be kept for ten years after training completed3Other training records - keep for six years after training completed.

Procurement	Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Procurement	Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	
Estates	Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
Estates	CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Estates	Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Estates	Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	

Estates	Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Estates	Leases	Termination of lease	12 years	Review and if no longer needed destroy	
Estates	Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	
Estates	Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Estates	Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	
Estates	Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Nynhydrin Test	Date of test	11 years	Review and if no longer needed destroy	
Estates	Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of Deposit	
Finance	Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Finance	Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. Where benefactions endowment trust fund/legacies - permanent retention.
Finance	Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	

Finance	Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible
Finance	Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Finance	Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Finance	Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Finance	Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Finance	Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.

Legal, Complaints & information Rights	Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
Legal, Complaints & information Rights	FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Legal, Complaints & information Rights	Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	
Legal, Complaints & information Rights	Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/action	Lifetime of patent or 6 years from end of licence /action	Review and consider transfer to Place of Deposit	
Legal, Complaints & information Rights	Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Subject Access Requests (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Subject access requests where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	

14 APPENDIX F: MAINTAINING RECORDS

14.1 Retrieving Archived Records

If the electronic system indicates that there is history and you require historical records for this service user then:

- Request the file from Archives via the Records.Requests@bdct.nhs.uk address.
- Archives will return all known files for the service user or staff member to the requester or scan them onto the relevant patient database.

Filing and Storage of Personal or Sensitive Paper Records

Where paper records are held locally adequate space and secure storage must be made for all service user and staff paper records held locally.

Do Not:

- Remove individual pieces of paper to make more room in a volume (unless these are print-outs from Trust clinical system or photocopies of the same).
- Pack records tightly into spaces, as this will damage them, papers and file covers may become loose and torn, rendering information illegible. Damaged and illegible records may increase the risk of harm to service users.
- Store duplicate copies of notes, for example, print outs from SystmOne.

Do:

- Remove a whole volume to archive storage or for secure destruction.
- Make more space available, and where possible, send records to archives for storage.

All type of Records created by the NHS **must** be retained for a minimum period of time. BDCFT has adopted the national guidance from the ***Records Management Code of Practice for Health and Social Care.***

Archiving Paper Records Procedure

Person/Team Responsible

Record Holder

1. Contact the Records Management Team on 01274 322060
Email: Records.Requests@bdct.nhs.uk

2. Complete the spreadsheet provided by the RM team
Name, date of birth and NHS number for each service user

3. Pack the boxes provided

Please ensure the following:

- each box weighs no more than 15kg as they have to be lifted on and off shelves.
- duplicated, copied or downloaded information is removed before you put files in boxes (print-outs from a clinical system for example). These copies should be shredded.
- files are stored standing upright in the boxes.
- you mark each box with a number and a title eg Box 1, Daisy Hill House: you must record this information on the spreadsheet for each record.

4. Send your completed spreadsheet to
Records.Requests@bdct.nhs.uk
prior to arranging the removal of the records from your site.

5. Keep a copy of your spreadsheet

Records Management

1. Provide spreadsheet for completion.
2. Provide boxes for storing and transporting the records.
3. Store records securely for the recommended retention period.
4. Destroy records when they have exceeded the recommended retention period.
5. Maintain a list of records held and records that have been destroyed.
6. Inform the relevant department when records are due to be destroyed.

Only original records should be sent to archives.
Please remove any copies, duplicated materials and print-outs from clinical or corporate systems.

Training, advice and guidance sessions are available from the Information Governance and Records Management Team:
IG.Department@bdct.nhs.uk

Further information and guidance documents can be found on the Information Governance pages on **Connect.**

14.2 Information Security

Advice and guidance for keeping information secure can be found in the **Information Security policy** and related procedures.

14.3 Records Transfers

14.3.1 Internal Post

For internal requests, the following good practice must be in place:

- Files must be double wrapped in two envelopes.
- The recipient’s name and full address must be written on both envelopes.
- A “return to sender” name and address must be written on both envelopes
- A “private and confidential” notice must be placed on both envelopes
- Placed in a coloured mail bag

14.3.2 External NHS Requests for Paper Records

There will be times when BDCFT records are requested by other NHS Organisations. Primarily these are other NHS Organisations who are now providing care to one of our service users who has moved into their area or has been transferred to care outside of BDCFT

If you receive a request from another NHS organisation for a service user’s records, you must contact the IG&RM team who will fulfil the request: records.requests@bdct.nhs.uk

The IG&RM team will check with the hospital/service concerned that they do need them and that the service user is currently being treated by them.

If it is established that the notes are needed by another NHS Trust, the IG & R team will: send digital records by secure transfer.

14.3.3 External Post

Records may be transferred

- by hand
- an approved courier service
- special delivery by the post office

Please note: The transfer of Records by taxi should be used as an emergency measure only. Notes must always be taken to their destination by a member of staff and not left with a taxi driver. The sender must only use a Trust-approved and contracted Taxi firm. Details of those firms are available from Supplies.

14.3.4 Emails

All email addresses that end with the following are deemed secure:

@bdct.nhs.uk	Bradford District Care NHS Foundation Trust
@nhs.net	NHSmail addresses
@pnn.police.uk	Police National Network/Criminal Justice Services secure email domains
@cjsm.net	Police National Network/Criminal Justice Services secure email domains
@gsx.gov.uk	Government secure email domains
@gse.gov.uk	Government secure email domains
@gcsx.gov.uk	Local Government/Social Services secure email domains
@gsi.gov.uk	Government secure email domains
@scn.gov.uk	Government secure email domains

For emails that end in the above addresses we are able to send/receive emails without the need for additional WinZip/password protection.

In addition to the above, published on the NHS Digital website is a list of other NHS Trusts that also meet this requirement NHS Digital Secure Email Standard

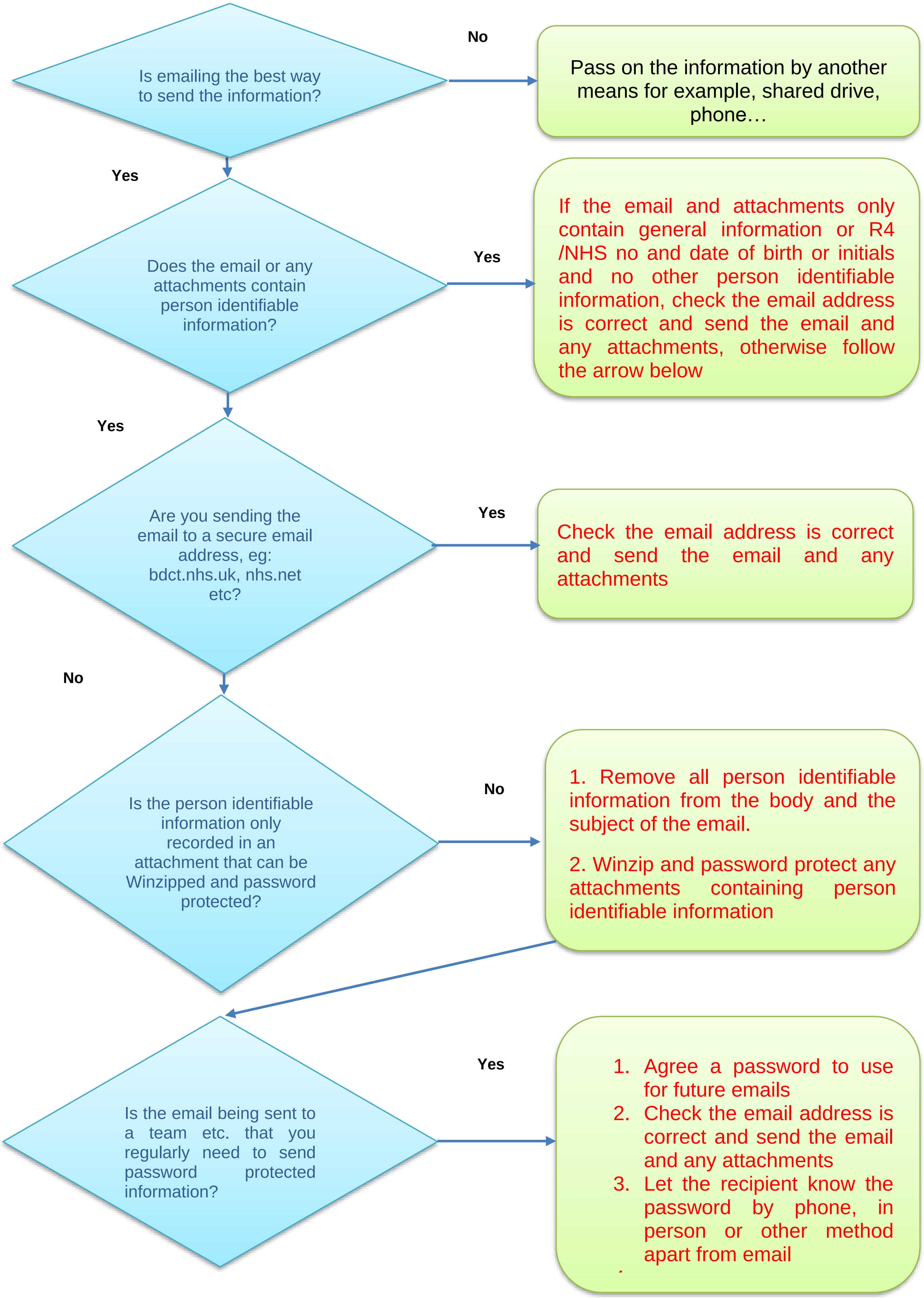
Any emails sent with sensitive/personal information to any other email address/individual/organisation, please continue to WinZip and password encrypt in the same manner, as we cannot guarantee the safety of the information on the recipient's systems.

With Agile working we are all likely to use emails far more but there are things we must all consider:

- Using email to share or discuss personal information is risky, primarily because it is so easy to type in or select the wrong address
- Before emailing confidential information always consider other ways of sharing the information
    - via clinical systems
    - shared drives
    - telephone

  - face to face discussions

- If you think that it’s absolutely necessary to email personal information (where an individual is or can easily be identified) and you are emailing to a non-secure address (hotmail, gmail etc.), you must ensure the personal information is held in an encrypted and password protected attachment rather than the body of an email. This way only staff with a legitimate right of access will have the password to open it.
- Use ‘Winzip’ and apply a password to encrypt and protect the attachment. If you’re not sure how to do this there is guidance on connect on the IT Service Desk pages (under IT documents)
- Provide the password to open the attachment by a different means (not email), e.g. a phone call, in person or by Lync
- If you or your colleagues are emailing to the same address on a regular basis, eg a Children’s Centre or within your team, then you and the recipients can agree a password in advance and use this each time
- Only 2 pieces of personal identifiable information can be contained in the body of an email or in the subject bar, for example, NHS number plus initials.



Is emailing the best way to send the information?

No

Pass on the information by another means for example, shared drive, phone…

Yes

Does the email or any attachments contain person identifiable information?

Yes

If the email and attachments only contain general information or R4 /NHS no and date of birth or initials and no other person identifiable information, check the email address is correct and send the email and any attachments, otherwise follow the arrow below

Yes

Are you sending the email to a secure email address, eg: bdct.nhs.uk, nhs.net etc?

Yes

Check the email address is correct and send the email and any attachments

No

Is the person identifiable information only recorded in an attachment that can be Winzipped and password protected?

No

1. Remove all person identifiable information from the body and the subject of the email.

2. Winzip and password protect any attachments containing person identifiable information

Is the email being sent to a team etc. that you regularly need to send password protected information?

Yes

1. Agree a password to use for future emails
2. Check the email address is correct and send the email and any attachments
3. Let the recipient know the password by phone, in person or other method apart from email

You must exercise caution when emailing information that, even if indirectly, identifies someone's medical condition or other issues. This will also be the case if no direct reference to an illness or condition is made. For example the following message:

> *'Dear Mrs Jones*
>
> *I will visit you on 1st July at 11 AM to change your dressings.*
>
> *Yours Mrs A District Nurse*
>
> *Bradford District Care NHS Foundation Trust'*

This message indicates that Mrs Jones has a medical condition that is being treated by a health professional. The email would have been fine if Mrs Jones's name had been omitted, or the letter just contained details of the appointment time and date. In this case had the email gone to an unintended recipient no service user sensitive information would have been disclosed.

There is no problem with emailing information leaflets or other publically available information.

14.4 Building Closure Checklist

Note: This form must be filled in when staff are vacating a building. The Service Manager and Estates and Facilities hold joint responsibility for the completion of this document.

Name & Address of Building:		
Service Lead:		**Contact No:**
Estates and Facilities Lead:		**Contact No:**
Date of Pre-Start:		**Alarm Code:**

Future of Building	
Is the building going to be reused at a later date?	Yes / No
Is the building going to be demolished / disposed?	Yes / No
Has a Risk Assessment been carried out?	Yes / No

Actions Following Risk Assessment	
Final meter readings- Electricity	
Final meter readings- Gas	
Final meter readings- Water	
Fire detection system	
Intruder Alarms set (consider effects of cutting off electricity)	
Security System e.g. remote door entry telecom and CCTV etc.	
Inform insurance company as policy may change for closure or cancelled for demolition.	
Are routine inspections planned?	Yes / No
Have key holders been notified?	Yes / No
Have the Police been given key holder details?	Yes / No
Has the planning authority been consulted?	Yes / No
Have all H&S files, Asbestos log, Legionella and Fire Risk Assessments been handed over to the Facilities Department?	Yes / No
Have all Maintenance checks been completed?	Yes / No
Additional security measures required: e.g. letter boxes sealed up etc.	
Asset Inventory completed?	Yes / No
Have Payroll/HR/Finance been informed?	Yes / No

14.5 Inspection Schedule

Directorate:……………………………………..

Decomissioning of:……………………………………….

Inspection Lead:………………………………..

Name	Designated Area

Following inspection I can confirm that the accommodation listed below has been cleared of all business documents and health records containing person identifiable information. The building is safe and secure and has been closed down in accordance with Estates guidance.

Floor	Room Number	Description	1st Inspection date	Comments	Actions	2nd inspection date	Comments	Actions	Date confirmed clear

15 APPENDIX G: USE OF RECORDS

15.1 Service User Records

The purpose of the record is to:

- provide a factual, chronological, comprehensive, concise and justifiable written account of care, treatment and support provided or planned for a service user.
- provide an accurate and intelligible account of the aims and main developments of any treatment over a given timescale
- assist in the continuity of care
- record an initial assessment of the service user and their situation
- communicate with other health/social care professionals, describing what has been observed or done (or not done) with the reason why
- to record the outcomes of any therapy from the viewpoint of both the service user and the therapist
- provide evidence of care, treatment and support required, intervention by practitioners, feedback on progress and service user responses
- Provide recommendations and plans for further contact and other forms of treatment, including health promotion and prevention
- provide a record of any problems that arise and the action taken in response to them
- record any factors (physical, psychological, social or spiritual) that may affect the service user
- record the effectiveness and outcome of interventions and to provide a baseline record against which improvement or deterioration may be judged
- record the chronology of events and the reasons for any decisions made
- provide information for clinical management, self-evaluation / reflective practice, clinical audit, quality assurance, research and resource management and to support standard setting
- meet minimum legal requirements and recommended guidelines
- meet professional and statutory requirements for record keeping

15.2 What to record

- Records must reflect that reasonable actions have been taken in:
- assessment and identification of the service user's problems / needs
- planning the expected outcomes and the interventions required to achieve it
- putting the planned interventions into practice
- evaluating the actual outcome against the expected outcome and changing the care plan / treatment plan / person centred plan / intervention / therapeutic goal where required
- assessing each child who visits in line with the Trust's Children Visiting policy and decisions are documented in the notes and the care plan, if appropriate
- Details of all multi-disciplinary interventions carried out and contact with the service user by professionals working with the service user will be recorded in a contemporaneous record.

Examples of interventions that should be included would be:

- Instructions for treatments, therapies, service provision
- Medication prescribed, given and omitted, including routes, amount, time of administration and the signature of the member of staff administering the medication
- Records of treatments and therapies given and omitted, including the type of therapy, the amount or duration of therapy, the time the treatment or therapy was carried out and the signature of the member of staff carrying out the treatment or therapy. While therapy is on-going, information regarding contacts carried out and failed contacts
- Specimens ordered including type, time and whether or not they were obtained
- A record of doctor's visits to the service user including contacts with attempts to contact the doctor making it clear whether or not the person was seen and examined in person, and noting any outcomes or interventions/changes required as a result
- Informed, specific consents obtained for treatments, chemotherapy and other special procedures or treatments (further guidance on this is contained in the BDCFT Consent Policy).
- In art psychotherapy a consent form for the service user's approval of the art work being photographed for record purposes, and for use of images in an educational context
- Invasive interventions such as the insertion and/or the removal of catheters, percutaneous endoscopically-guided gastrostomy (PEG) feeding tubes, sutures etc.
- Information and education provided to the service user, carers or family including instructions on care, medication, treatments and dietary requirements
- A discharge summary containing instructions and information given to the service user, their carers/family, social staff, community nurses, the GP and any other service the service user was attending / referred to prior to the current admission or referral. The summary should also contain an overall appraisal of any therapy the service user received.

Progress notes should be written up at least once per span of duty (In-Service user, residential and supported accommodation areas), and/or at each contact with the service user (Allied Health Professionals, Psychologists, Therapists and Social Staff) and could include:

- A review of the service user's condition/progress/the course of therapy and its main developments (both positive and negative) and considerations relating to the timescale of treatment
- Responses to treatment/intervention and/or medications
- Plans for further care/intervention/appointments
- A record of discussions with the service user, carers or family members
- A record of discussions with doctors, Allied Health Professionals or other health/social care providers
- ECT, laboratory, x-ray and other diagnostic test results
- Incidents, accidents, injuries sustained, infections contracted while in hospital, medication incidents and errors (including refusal to take prescribed medications) and follow up care provided. IR-e numbers must also be recorded in the progress notes

- Service User responses to treatment/therapy/interventions
- Service User's specific refusal to co-operate or follow prescribed plans of care including leaving the hospital/care setting against medical/professional advice

As a minimum, progress notes must include date, time, a short description of why the person was seen, any information which materially changes the risk assessment or care plan and advice to the care team on how to deal with the person in the short and medium term.

15.3 Statements and Allegations

When quoting statements or allegations they must be attributed to the person they were made by. Resulting actions must be recorded. Where an allegation leads to use of other policies (such as the Complaints Policy, Incident Management Policy or Disciplinary Policies) they should be referenced in the service user's record. Specific details of investigations will not, however, be mentioned in the service user's record.

The record should also contain:

- All letters and reports relating to the service user, including a record of where copies of these letters and reports were sent
- All correspondence for service users going out of the Trust to external sources must contain the service user's NHS number
- Internal correspondence should also use the service user's NHS number, as best practice dictates
- Evidence that the service user has received copies of all letters sent to and about them. (BDCFT Policy on Copying Correspondence to Service Users) Where the service user has consented to, or opted not to, receive such letters, this is recorded, and where it is not felt appropriate for the service user to receive letters this is also recorded
- Notes of any contact with other professionals relating to the service user during the course of treatment/therapy
- The service user's own evaluation of any therapy they are receiving
- In the case of a failed therapy or a decision to terminate any therapy prematurely, the therapist's understanding of the situation, as well as the service user's (if available)

All contacts with service users MUST be recorded in their case notes. We must not be reliant on other sources to record our contacts.

ANY and ALL clinical investigations that are ordered must be recorded in the service user's notes. The subsequent results should be discussed with the service user, and there MUST be a note in the records to show as much, that the investigations were ordered and the results discussed with the service user.

Retrospective entries can be included, however it must be stated that this particular entry is a retrospective entry, and the reason why it is so must also be recorded.

For further guidance and support on giving statements, the Royal College of Nursing has produced a guide: Guide, or on Connect: Guide

15.4 Wellbeing of Children and Young People

Service user records must promote the health, wellbeing and safety of any children and young people with whom the service user is in contact

Service user records should be able to support the protection of children and vulnerable adults from significant harm. Please refer to the Safeguarding policies and procedures for further guidance

Service user records should include:

- clear details of children for whom the service user has responsibility

- clear details of the service user's main carer or next of kin

All exceptions to this standard identified by staff should be reported to their line manager.

15.5 Non-Qualified Staff

Trained staff should assess the ability of staff who they are responsible for as part of induction/supervision/appraisal and ensure delegation to write records is consistent with capability and capacity.

The responsible staff member should assess through a regular audit of a sample of entries whether the competence is assessed accurately.

Staff should not complete entries unless authorised to do so by their line manager after assessment of competence.

Staff should not access or complete entries on any electronic system unless they have received the appropriate training and possess their own unique password and/or smartcard

Qualified staff members who counter-sign or verify unqualified staff entries, must also adhere to the standards above.

Where a registered clinician delegates record keeping to a student or support staff, they must ensure that the person is competent for the task and adequately supervised.

A large number of support staff working in clinical and care areas for whom maintaining accurate records is part of their substantive post. They have a duty to adhere to this policy.

If the qualified staff member has concerns regarding the quality or accuracy of an entry, they should challenge the author of the entry and ask them to amend it as necessary. It should not be approved until they feel the entry is acceptable.

All non-service user records (e.g.: Finance, Personnel, Estates and Facilities) must also be treated with respect and the due care and attention they demand.

16 APPENDIX H: RECORD DISPOSAL

16.1 Permanent Preservation

All records created by BDCFT need to be effectively managed, and this includes their disposal and destruction, regardless of the medium in which they are held.

It must not be assumed that all records will be automatically destroyed at the end of their minimum retention period as outlined in **Records Management Code of Practice for Health and Social Care**.

Some records will have historical value, either social or political, and may be required for permanent preservation at the approved Place of Deposit, situated in Wakefield, managed by the National Archives (NA, formerly the Public Records Office). Responsibility for the National Archives lies with the Department for Constitutional Affairs.

The maximum time limit a Trust can keep records for is thirty years from the last time information was added (ie: if the last contact with a service user was 2005, then the record can be kept by BDCFT until 2035).

ALL records which are thirty years old or more must, by law, be offered to the National Archives (NA). This is because the records become the property of the Lord Chancellor at thirty years old.

Any person encountering records which are over thirty years old is committing a criminal offence under the Public Records Act, if they do not offer them to the NA before they destroy them.

Not all records will be preserved by the NA. Those records which the NA deem not worthy of preservation can be destroyed confidentially, either by the Trust or the NA (this can be agreed by the two parties and can vary on a case by case basis). All records destroyed by BDCFT must be listed. This list must be kept for thirty.

Below is a bullet point list outlining the Permanent Preservation process:

- Request is made to the Information Governance and Records Manager for assessment.
- Records are assessed by the Information Governance and Records team.
- If the records are over thirty years old since last use/entry, then the Information Governance and Records team will contact West Yorkshire Archive Service (on behalf of NA) for an appraisal.
- If WYAS agree to take them, they will be acceded to their nearest repository, which is situated in Wakefield.
- The Trust will receive a list of records acceded to NA, and each deposit made to them is signed to show agreement between NA and BDCFT. (The Information Governance and Records Manager signs on behalf of BDCFT).

The above only applies if Records are acceded in the course of time. If there are no accessions, then there will be no evidence of transfer to NA.

16.2 Disposal

The retention periods stated in **Records Management Code of Practice for Health and Social Care**, have been adopted by BDCFT and are used accordingly. Please refer to **Procedural Appendix E:** Record Retention within this document.

The Trust will in some circumstances, retain records for an additional period of time to further assure the record is no longer required. For example, in the case of deceased service users: DH guidance states these records must be kept for a minimum of eight years. BDCFT has made the decision to keep them for ten years before destruction.

16.3 Destruction of Records

- Destruction of Records is an irreversible act, and must not be undertaken without the involvement of the Information Governance and Records Management team.
- The willful destruction of public Records is a criminal offence. Any records destroyed without appropriate authorisation may be deemed willful destruction.
- Destruction of all Trust records must be carried out by a Trust approved contractor.
- A list must be made of **all** records destroyed. This must be sent to the Information Governance and Records Management team to update the central database of destroyed records. A local list may also be kept for reference purposes.
- This listing is a requirement under the Public Records Act 1958 and also the Records Management: Code of Practice.
- All records marked for confidential destruction with the Trust's approved contractor must be put in destruction sacks marked with their logo.
- Records marked for destruction must be placed in the Trust's approved contractors confidential waste bags, and tied shut, to prevent accidental disclosure.

When filling these bags it is acceptable to mix contents if the following is completed. The list must include:

- Contractor's tie number (this is unique)
- Contents (general heading are fine, for example, Diaries)
- Period the records cover (1994-98)

Once collected, the bags will be confidentially shredded within 48 hours.

To comply with the Data Protection Act, the Information Governance and Records team will obtain an electronic Certificate of Destruction from the contractor, as proof the records have been destroyed securely. A copy of this certificate is available on request.

The serial number on this certificate will be added to the destruction database. Paper records can be destroyed to an international standard. They can be incinerated, pulped or shredded (using a cross cut shredder) under confidential conditions.

No information can be destroyed if it is the subject of a request under the Data Protection Act and/or Freedom of Information Act or any other legal process, such as an inquest following a death.

17 APPENDIX I: HOW TO DEAL WITH SPECIFIC TYPES OF RECORDS

17.1 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.

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 care records, it may be necessary to inform the individuals concerned about the change. 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 DPA 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.

17.2 Records at Contract Change Scenarios:

Characteristic of new service provider	Fair processing required	What to transfer?	Sensitive
NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light- notice on appointment letter explaining that there is a new provider. Local publicity campaign such as signage or posters located on premises.	Entire record or summary of entire caseload.	N/A
Non NHS provider from same premises and involving the same staff. This may be a merger or	Light - notice on appointment letter explaining that there is a new provider. Local	Copy or summary of entire record of current caseload. Former provider retains the original	N/A

regional reconfiguration.	publicity campaign involving signage and poster and local communications or advertising.	record.	
NHS provider from different premises but with the same staff.	Light - notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	N/A
NHS provider from different premises and different staff.	Moderate - a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	Individual communications may not be possible so consent of current caseload may need to be sought before transfer. It may not be possible to transfer the record without explicit patient consent so in some cases no records will be transferred.

17.3 Complaints Records

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

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 ICO has issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

17.4 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. 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.

17.5 Adopted Persons Health Record

Notwithstanding any other centrally issued guidance by the DH 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.

17.6 Health Records of Transgender Persons

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 200467.

The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient.

It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

17.7 Witness Protection Health Records

Where a record is that of someone known to be under a witness protection scheme, the record must be subject to greater security and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the Courts for the purposes of identity. The right to anonymity extends to medical records.

For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

17.8 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 care records. Where the asylum seeker is given a patient held record, th provider must satisfy themselves that they have a record of what they have done in case of litigation or matters of professional conduct.

17.9 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.

18 APPENDIX J: RECORDS SECURITY: WORK BASE, HOME WORKING, AGILE WORKING

- All person identifiable data or commercially sensitive data must be saved with appropriate security measures. Staff must not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of the Trust. The only equipment that you should use will be supplied by the Trust. This equipment will have the appropriate security software and encryption applied. It is important that you take reasonable and common sense measures to protect equipment.
- Person identifiable data should not be stored on any removable media, however if there is no other option, ensure this data is stored on a corporate encrypted device and deleted once transferred to an identified secure area folder.
- When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.
- When transferring data either directly or via a third party, ensure security measures and precautions have been actioned by the sender and receiver.
- A robust information sharing contract should be in place detailing responsibilities. Please contact the Information Governance and Records Management team for more advice.
- Never leave your computer logged on when unattended.
- You must not leave your smart card in a device when the device is not in use or if you are elsewhere for example, in a meeting.
- If you lose your smartcard you should report this immediately to your line manager and complete an incident report (IRE).
- If you are emailing a non-secure address (hotmail, gmail etc.) always use Winzip software to encrypt and password-protect any attachments that contain confidential or sensitive data. Staff must send the password via alternative means – ie not by email. There is no need to winzip if you are sending another secure email address eg NHS.net, @pnn.police.uk, @cjsm.net, @gsx.gov.uk

If you notice anything suspicious whilst using the network please report it to the service desk: servicedesk@bdct.nhs.uk or 01274 251251.

The Information Security Policy is available on Connect.

18.1 Agile Working

- Make sure when you leave a room or building you have all equipment with you
- Ensure your vehicle is locked and windows closed
- Park in a safe place
- If you need to leave equipment in your car for a short period make sure it is out of sight e.g. in a boot or glove compartment.
- Do not leave devices or information in a car overnight.
- If any equipment is stolen you must report this to the police, your line manager, and IT. An incident report will need to be completed before a replacement device can be issued.
- Always be aware of who is around you, and what they can see, when you are updating records in a public place. Try and choose a seat in a corner or by a wall in a café/public place so no one can sit behind you.

- Where information is available electronically – e.g. diary, appointment lists etc. this should be accessed electronically and paper versions should not be created.
- If there is a need to transport paper records you must ensure these are secure and that confidentiality is maintained. This is of particular importance if you leave records in your car during visits etc. Paper records should be stored out of sight and be secured e.g. in the boot
- Make sure paperwork is not left in someone's home or in a public place
- Do not leave paperwork where other people can see it e.g. face up on a car seat.

In the rare circumstance that information isn't available electronically paper records can be taken home ready to use the next working day, but cannot be left in car overnight. All paper based documents need to be stored securely within the staff member's home.

For community services who visit patients in their own home rather than printing off a "visit list" it is expected that a local copy of the diary/schedule is saved on the desktop and deleted within 24 hours. The information should be minimised to a single day's schedule. Data recorded should still be kept to a minimum, with codes used for treatment interventions and key codes should be recorded separate to service user names.

Staff may use a Word document to make notes during a clinic or home visit when inputting detailed notes into the clinical system record is too time consuming, and/or would have an impact on the interaction between the staff member and the service user. This should always be saved into a personal or shared service drive, not on the laptop home page. The clinical record should then be updated as soon as possible afterwards (and up to a maximum of 24 hours as per record keeping policy) and the Word document then immediately delete and the recycle bin emptied (the recycle bin is available on the desktop).