Records management policy
CG16

Beware when using a printed version of this document. It may have been subsequently amended. Please check online for the latest version.

Applies to:	All NHS Resolution employees
Version:	V3_8 final
Date of SMT approval:	6 November 2019
Review date:	November 2022
Author:	Tinku Mitra
Owner:	Joanne Evans

Contents

1. Introduction

1.1. Records management is the process by which an organisation manages all aspects of its records, whether internally or externally generated and in any format or media type, from their creation all the way through their lifecycle to their eventual disposal.

1.2. NHS Resolution'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, and protect the interests of the organisation and the rights of claimants and appellants, staff and members of the public. They support consistency, continuity, efficiency and productivity, and help deliver services in consistent and equitable ways.

1.3. This policy sets out an overarching framework for integrated records management at NHS Resolution. It is intended to ensure the confidentiality, integrity, availability and effective use of records, thus enabling overall co-ordination of records management activities for alignment with business strategy and statutory and legal obligations, including the relevant requirements of The General Data Protection Regulation (EU) 2016/679) and national laws implementing GDPR (together "GDPR"), and the Freedom of Information Act 2000.

2. Definitions

2.1. In this policy, 'records' are defined as 'recorded information, in any form, created or received and maintained by NHS Resolution in the transaction of its business or conduct of affairs and kept as evidence of such activity'. This policy relates to all records held in any format by NHS Resolution as per the Department of Health and Social Care (DHSC) publication Records Management: NHS Code of Practice, i.e.:

- all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints etc);
- all claim, appeal and dispute files; and
- all records associated with the business of all NHS Resolution departments.

2.2. 'Information' is a corporate asset. NHS Resolution's records are important sources of administrative, evidential and historical information. These include records held in all formats, for example:

- paper records, reports, diaries and registers etc;
- electronic records;
- images;
- microform (i.e. microfiche and microfilm); and
- audio and video tapes.

2.3. They are vital to NHS Resolution to support its current and future operations (including meeting the requirements of Freedom of Information and Data Protection legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

2.4. The term 'records life cycle' describes the life of a record from its receipt/creation through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

3. Legal and professional obligations

3.1. All NHS records are Public Records under the Public Records Act. NHS Resolution will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- GDPR
- The Data Protection Act 2018
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

and any new legislation affecting records management as it arises.

3.2. GDPR requires organisations which hold 'personal data' to meet certain minimum standards in the way they process that data. It does not prevent the storage or use of data, but sets standards as to how this is to be done. It also permits the individuals who are the subject of any data ("data subjects") to gain access to that data, although with a number of exemptions. Details are provided within CG14 – *Data protection policy*.

3.3. The Freedom of Information Act 2000 (FOIA) gives a general right of access to recorded information held by public authorities, sets out exemptions from that right, and places a number of obligations on public authorities such as NHS Resolution. Details are provided within CG15 – *Freedom of information policy*.

4. Duties

4.1. Chief Executive

The Chief Executive has overall responsibility for records management. As accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and business continuity. This covers all information governance matters including compliance with the requirements of the *Records management policy*.

4.2. Director of Finance and Corporate Planning

The Director of Finance and Corporate Planning is the Senior Information Risk Owner (SIRO) and as such has overall responsibility for the management of risks associated with the handling of information, especially the use of personal identifiable information, and is responsible for ensuring that information is shared in an appropriate and secure manner.

4.3. Information Governance Manager

The Information Governance Manager is responsible for the day-to-day oversight of records management issues and for ensuring that records are handled in accordance with NHS Resolution policy and legal requirements.

4.4. Information Governance Group

The IG Group will have responsibility for reviewing IG risks and incidents and for oversight of all operational and strategic IG matters. The SIRO will sit on this group and a summary of the minutes will be circulated to the Audit Committee.

4.5. Head of IT & Facilities

As the Information Security Officer, the Head of IT & Facilities has overall responsibility for the provision of systems and facilities to support accurate, legally compliant, secure and efficient information governance.

4.6. Information Asset Owners

Information Asset Owners are responsible for identifying risks in respect of records pertaining to their departmental function and are responsible for addressing those risks in conjunction with the Corporate Governance Team.

4.7. Line managers

All line managers are responsible for the promotion of the principles outlined within this policy and associated policies, within their teams, inclusive of all direct employees, temporary agency staff and contractors.

4.8. Employees

All employees, temporary agency staff and contractors are responsible for the implementation of the principles outlined within this policy and associated policies and for reporting any related adverse incidents in line with CG11 – Incident Reporting Policy and Procedure. All employees must be aware of NHS Resolution's legal and statutory obligations in respect of records management, and ensure that these obligations are met.

5. Robust records management

The key elements of NHS Resolution's management system are to ensure that:

- records are available when needed;
- records can be accessed - and that the current version is identified where multiple versions exist;
- records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- records can be maintained through time – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- records are secure - that access and disclosure are properly controlled;

- records are retained and disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management.

6. Information assets

It is the responsibility of Information Asset Owners (IAOs) to identify key information assets which are of value to the specific function and/or wider organisation. Key information assets will be entered onto the Information Asset Register (IAR).

7. Information risk assessment

IAOs are responsible for ensuring that information risk assessments are:

- performed for all information assets for which they are responsible
- performed as part of project proposals
- up-to-date and reported to the SIRO
- reviewed when information systems or processes are altered or amended

8. Information asset register

NHS Resolution aims to have an established and up-to-date IAR, which is an inventory of all key information assets. The IAO must ensure that their portion of the IAR is completed to include:

- the identification and addition of all key records held within their remit
- the location
- the categorisation
- the format
- the classification
- the identification of the IAO responsible
- reference to third party access
- details of the risk assessment
- the controls/safeguards (current and/or required)
- the dependencies
- the archiving and disposal arrangements

9. Retention and disposal schedule

9.1. It is a fundamental requirement that all of NHS Resolution's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to NHS Resolution's business functions.

9.2. NHS Resolution has adopted the retention periods set out in the Records Management: NHS Code of Practice. The retention schedule will be reviewed whenever records management legislation changes or new organisational practices are implemented. The current retention and disposal schedule can be found in Appendix 1.

10. Training and support

All NHS Resolution staff will be made aware of their responsibilities for record- keeping and record management through generic and specific training programmes and guidance. IAOs will receive specific training on the IAR and other concepts and tools associated with records management. All relevant training will be arranged and monitored through the Information Governance Group.

11. Monitoring effective implementation

11.1. NHS Resolution will regularly audit the implementation of aspects of this policy. The audit will:

- Identify which areas of operation should comply with this policy;
- Check the compliance of those areas with this policy;
- Lead to a subsidiary development plan if there are major changes to be made;
- Lead to the adjustment of this policy and re-iteration of the requirements therein, as necessary.

11.2. The results of the records management systems audit will be reported to NHS Resolution Board. This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

11.3. The effective implementation of this policy will also be monitored by the Information Governance Group through review of a range of key performance indicators, including compliance with the requirements of the HSCIC Information Governance Toolkit, related incidents reported and risks arising on team and organisational risk registers (and associated actions taken), and by NHS Resolution Board through review of actions taken in response to requests made under the FOIA and DPA.

12. Related policies and procedures

CG11	Incident reporting policy and procedure
CG14	Data protection policy
CG15	Freedom of information policy
ITFA02	Procedure/guidance for working with confidential or sensitive information
	Privacy notice

13. References

- NHS Records Management: Code of Practice 2006
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (2009)
- Information Governance Alliances' Records Management Code of Practice for Health and Social Care 2016.

14. Document control

Date	Author	Version	Reason for change
04 April 2018	Evelyn Lucien	V3_8	Rebranding and change to NHS Resolution
30 May 2018	Katherine Ogilvie	V3_8	To include clear online publishing period within Appendix 1
20 July 2018	Julian Marku	V3_8	Updates to new service titles
14 June 2019	Adrienne Blackwood	V3_8	Updates to retention dates
1 December 2020	Tinku Mitra	V3_8	Amendment to Appendix 1

Appendix 1

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
ADMINISTRATIVE (CORPORATE AND ORGANISATIONAL)		
Advance letters (e.g. DHSC guidance)	6 years	
Agendas of board meetings, including groups In scheme of delegation (master copies, including associated papers)	20 years	Return to archive
Agendas (other)	2 years	
Annual reports presented to parliament	Permanent	
Parliamentary questions, MP enquiries	10 years	Destroy under secure conditions
Audit Records (e.g. Organisational Audits, Records Audits, Systems Audits) – Internal & External in any format (paper, electronic etc)	2 years from the date of completion of the audit	
Business plans, including local delivery plans	20 years (3 years online)	
Commissioning decisions Appeal documentation Decision documentation	6 years from date of appeal decision (3 years online) 6 years from date of decision (3 years online)	Destroy under secure conditions
Complaints - Correspondence, investigation and outcomes Returns made to DHSC	10 years from completion of action Files closed annually and kept for 6 years following closure	Destroy under secure conditions
Contracts	Permanent if current (7 years if expired)	
Copyright declaration forms (Library Service)	6 years	Destroy under secure conditions
Diaries (office)	1 year after the end of the calendar year to which they refer	Destroy under secure conditions
Flexi working hours (personal record of hours actually worked)	6 months	Destroy under secure conditions
Freedom of Information requests	3 years after full disclosure (3 years online); 6 years if information is redacted or the information requested is	Destroy under secure conditions
Legal advice	10 years	Destroy under secure conditions
Performers List Regulations enquires	6 years	Destroy under secure conditions
Health and safety documentation	3 years	Destroy under secure conditions
History of organisation or predecessors, its organisation and procedures (e.g. establishment order)	20 years	Return to archive
Incident forms	10 years	Destroy under secure conditions
Indices (records management)	Registry lists of public records marked for permanent preservation, or containing the record of management of public records – 30 years File lists and document lists where public records or their management are not covered – 30 years	

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
Records/documents relating to any form of litigation	10 years Where a legal action has commenced, keep as advised by legal representatives	Destroy under secure conditions
Manuals – policy and procedure (administrative and clinical, strategy documents)	10 years after life of the system (or superseded) to which the policies or procedures refer	Destroy
Meetings and minutes papers of major committees and sub-committees (master copies)	20 years (3 years online)	Return to archive
Meetings and minutes papers (other, including reference copies of major committees)	2 years	Destroy
Nominal rolls	6 years (maximum)	Destroy under secure conditions
Papers of minor or short-lived importance not covered elsewhere, e.g. advertising matter, covering letters, reminders, letters making appointments, anonymous or unintelligible letters, drafts, duplicates of documents known to be preserved elsewhere, other documents that have ceased to be of value on settlement of the matter involved.	2 years after the settlement of the matter to which they relate	Destroy under secure conditions
Project files (over £100,000) on termination, including abandoned or deferred projects	6 years	Destroy under secure conditions
Project files (less than £100,000) on termination	2 years	Destroy under secure conditions
Project team files (summary retained)	3 years	Destroy under secure conditions
Receipts for registered and recorded mail	2 years following the end of the financial year to which they relate	Destroy under secure conditions
Records documenting the archiving, transfer to public records archive or destruction of records	20 years	Return to archive
Records of custody and transfer of keys	2 years after last entry	Destroy under secure conditions
Reports (major)	30 years (3 years online)	Destroy under secure conditions
Requests for access to records, other than Freedom of Information or subject access requests	6 years after last action	Destroy under secure conditions
Requisitions	18 months	Destroy under secure conditions
Research ethics committee records	3 years from date of decision	Destroy under secure conditions
Serious incident files	30 years	Destroy under secure conditions
Specifications (e.g. equipment, services)	6 years	Return to archive
Statistics (including Korner returns, contract minimum data set, statistical returns to DHSC, patient activity)	3 years from date of submission	Destroy
Subject access requests (DPA)– records of requests	3 years after last action/ 6 years where there was a review or ICO involvement	Destroy under secure conditions
Time sheets (relating to a Group or Department where the timesheets are kept as a tool to manage resources, staffing levels)	6 months	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
ESTATES		
Inventories of furniture with a minimum life of 5 years	Keep until next inventory	Destroy
Maintenance contracts (routine)	6 years from end of contract	Destroy
Manuals (operating)	Lifetime of equipment	Destroy
FINANCIAL		
Accounts – annual (final – one set only)	20 years	Return to archive
Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques (for cheques bearing printed receipts, see Receipts), accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records, laundry lists and receipts)	2 years from completion of audit	Destroy under secure conditions
Accounts – working papers	3 years from completion of audit	Destroy under secure conditions
Advice notes (payment)	1.5 years	Destroy under secure conditions
Audit records (internal and external audit) – original documents	2 years from completion of audit	Destroy under secure conditions
Audit reports – internal and external (including management letters, value for money reports and system/final accounts memoranda)	2 years after formal completion by statutory auditor	Destroy under secure conditions
Bank statements	2 years from completion of audit	Destroy under secure conditions
Banks Automated Clearing System (BACS) records	6 years after year end	Destroy under secure conditions
Bills, receipts and cleared cheques	6 years	Destroy under secure conditions
Budgets (including working papers, reports, virements and journals)	2 years from completion of audit	Destroy under secure conditions
Capital charges data	2 years from completion of audit	Destroy under secure conditions
Capital paid invoices (see Invoices)	(see Invoices)	Destroy under secure conditions
Cash books	6 years after end of financial year to which they relate	Destroy under secure conditions
Cash sheets	6 years after end of financial year to which they relate	Destroy under secure conditions
Contracts – financial	Approval files – 15 years Approved suppliers lists – 11 years	Destroy under secure conditions
Contracts – non-sealed (property) on termination	6 years after termination of contract	Destroy under secure conditions
Contracts – non-sealed (other) on termination	6 years after termination of contract	Destroy under secure conditions
Contracts – sealed (and associated records)	Minimum of 15 years, after which they should be reviewed	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
FINANCIAL		
Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract	6 years after end of financial year to which they relate	Destroy under secure conditions
Cost accounts	3 years after end of financial year to which they relate	Destroy under secure conditions
Creditor payments	3 years after end of financial year to which they relate	Destroy under secure conditions
Debtors' records – cleared	2 years from completion of audit	Destroy under secure conditions
Debtors' records – uncleared	6 years from completion of audit	Destroy under secure conditions
Demand notes	6 years after end of financial year to which they relate	Destroy under secure conditions
Estimates, including supporting calculations and statistics	3 years after end of financial year to which they relate	Destroy under secure conditions
Excess fares	2 years after end of financial year to which they relate	Destroy under secure conditions
Expense claims, including travel and subsistence claims, and claims and authorisations	6 years after end of financial year to which they relate	Destroy under secure conditions
Fraud case files/investigations	6 years	Destroy under secure conditions
Fraud national proactive exercises	3 years	Destroy under secure conditions
Funding data	6 years after end of financial year to which they relate	Destroy under secure conditions
Invoices	6 years after end of financial year to which they relate	Destroy under secure conditions
Ledgers, including cash books, ledgers, income and expenditure journals, nominal rolls, non-exchequer funds records (patient monies)	6 years after end of financial year to which they relate	Destroy under secure conditions
Non-exchequer funds records (i.e. funding received by the organisation that does not directly relate to patient care eg charitable funds)	30 years	Destroy under secure conditions
PAYE records	6 years after termination of employment	Destroy under secure conditions
Payments	6 years after year end	Destroy under secure conditions
Payroll (i.e. list of staff in the pay of the organisation)	6 years after termination of employment	Destroy under secure conditions
Positive predictive value performance indicators	3 years	Destroy under secure conditions
Receipts	6 years after end of financial year to which they relate	Destroy under secure conditions
Salaries (see Wages)		Destroy under secure conditions
Superannuation accounts	10 years	Destroy under secure conditions
Superannuation registers	10 years	Destroy under secure conditions
Tax forms	7 years	Destroy under secure conditions
Transport (staff pool car documentation)	3 years unless litigation ensues	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
Trust documents without permanent relevance/not otherwise mentioned	6 years	Destroy under secure conditions
VAT records	6 years after end of financial year to which they relate	Destroy under secure conditions
Wages/salary records	10 years after termination of employment	Destroy under secure conditions
IT		
Email System	6 years, (relates to data contained within the email system only)	Destroy under secure conditions
Extranet	6 years server images are retained	Destroy under secure conditions
HUMAN RESOURCES		
CVs for non-executive directors (successful applicants)	6 years following term of office	Destroy under secure conditions
CVs for non-executive directors (unsuccessful applicants)	2 years	Destroy under secure conditions
Industrial relations (not routine staff matters), including industrial tribunals	10 years	Destroy under secure conditions
Job advertisements	75 years	Archived
Job applications (successful)	6 years following termination of employment	Destroy under secure conditions
Job applications (unsuccessful)	2 years	Destroy under secure conditions
Job descriptions	75 years	Archived
Leavers' dossiers	6 years after individual has left Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time.	Destroy under secure conditions
Letters of appointment	6 years after employment has terminated or until 70th birthday, whichever is later.	Destroy under secure conditions
Pension Forms (all)	7 years	Destroy under secure conditions
Personnel/human resources records –major (e.g. personal files, letters of appointment, contracts, references and related correspondence, training records, equal opportunity monitoring forms (if retained))	6 years after individual leaves service, at which time a summary of the file must be kept until the individual's 70th birthday. Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time	Destroy under secure conditions
Personnel/human resources records – minor (e.g. attendance books, annual leave records)	2 years after the year to which they relate	Destroy under secure conditions
Study leave applications	5 years	Destroy under secure conditions
Timesheets (for individual members of staff)	2 years after the year to which they relate	Destroy under secure conditions
Training plans	2 years	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
PURCHASING / SUPPLIES		
Approval files (contracts)	6 years after end of the year the contract expired	Destroy under secure conditions
Approved suppliers lists	11 years	Destroy under secure conditions
Delivery notes	2 years after end of financial year to which they relate	Destroy under secure conditions
Suppliers records – minor (e.g. invitations to tender and inadmissible tenders, routine papers relating to demands for furniture, equipment, stationery and other supplies)	18 months	Destroy under secure conditions
Tenders (successful)	Tender period plus 6 year limitation period	Destroy under secure conditions
Tenders (unsuccessful)	6 years	Destroy under secure conditions
Practitioner Performance Advice		
EKS2 EKS2 case records	30 years (from last recorded case closure)	Destroy under secure conditions
Handwritten case notes For example, Adviser calls meetings etc.	Destroyed immediately after information added to EKS2	Destroy under secure conditions
Healthcare Professional Alert Notice (HPAN) HPAN Letters Database of Alert Notices	30 years	Destroy under secure conditions
Legal requests Requests for legal advice and advice received (not case-related)	Retain for lifetime of organisation Case-related advice will be added to EKS2 and then managed in line with EKS2 data.	Archive
Service feedback, analysis and evaluation All information relating to the administration and issuing of feedback requests (relating to our service). Feedback data, responses, analysis and aggregated reports.	10 years	Destroy under secure conditions
Activity reports Practitioner Performance Advice function activity reports and supporting data (including that supplied by Informatics).	30 years	Destroy under secure conditions
Contractor Products Multisource feedback (MSF): electronic data and reports	MSF is added to case record and managed in line with retention for EKS2 case data	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
Assessor workbooks Occupational Health (OH) reports Behavioral Assessment (BA) reports	Hard copy workbooks are scanned into EKS2 and then destroyed. Electronic records are then managed in line with EKS2 data OH reports are added to EKS2 and then managed in line with EKS2 case data. BA reports are added to EKS2 and then managed in line with EKS2 case data.	
Assessor Information Information held (outside of EKS2) on appointed assessors including details of areas of work; speciality and availability. Information relating to unsuccessful assessor candidates including application forms/CVs. Quality assurance and feedback about assessors, including outcomes of 360 degree feedback	Retained for 6 years after end of contract. Retained for 1 year after outcome of application process is notified. Retained for 6 years after submission of feedback.	Destroy under secure conditions
Quality Assurance Final reports of Quality Assurance exercises carried out by external contractors (for example, into Occupational Health and Behavioural Assessments).	10 years	Destroy under secure conditions
Primary Care Appeals		
Case Registry - case details	6 years after decision date	Destroy under secure conditions
File Management System	6 years from decision date	Destroy under secure conditions
Judicial Review Files	10 years from Judgment/Consent Order	Destroy under secure conditions
Case decisions (signed)	6 years from decision date	Destroy under secure conditions
FHSAA case decisions	6 years after decision date	Destroy under secure conditions
FHSAA (SHA) Board minutes and papers	30 years	Destroy under secure conditions
Fitness to Practise Checks	6 years	Destroy under secure conditions
Fitness to Practise Record	80th birthday of Performer	Destroy under secure conditions
Templates Standard letters Casework Procedure Notes	Until such time that current practice is established	Destroy under secure conditions
Panel member (unsuccessful) applications	6 months	Destroy under secure conditions
Panel member records	6 years after retirement/resignation	Destroy under secure conditions

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
CLAIMS MANAGEMENT		
Claims files (hardcopy) including CDs, disks, x-rays and any other media. (paper files) DTS	10 years after case closure	Destroy under secure conditions
Claims files relating to children and those with a disability (hardcopy) including CDs, disks, x-rays and any other media.	75 years after case closure	Destroy under secure conditions
Claims records held on Case Management System database	75 years after case closure (to be reviewed as part of case management system review)	Destroy under secure conditions
Claims procedures and protocols Admin procedures and protocols	Lifetime of the organisation plus 6 years	Destroy
Guidance notes	Lifetime of the organisation plus 6 years	Destroy
Technical training materials	20 years	Return to archive
Test cases which the NHS LA has a national overview (equal pay, discrimination)	10 years after case closure	Destroy under secure conditions
Log of Technical Claims Unit referrals	6 years after case closure	Destroy under secure conditions
Surveillance case log	6 years after case closure	Destroy under secure conditions
Audit logs	6 years	Destroy under secure conditions
GPI		
Scoping queries (email)	6 years after case closure	Destroy under secure conditions
Referral of cases that fall outside scope of CNSGP	6 years after case closure	Destroy under secure conditions
Process maps	Lifetime of the (organisation plus 6 years)	Archive
Standard operating procedures	Lifetime of the (organisation plus 6 years)	Archive
Template letters	Lifetime of the (organisation plus 6 years)	Archive
Call statistics from the helpline provider, money penny	6 years	Destroy under secure conditions
SAFETY AND LEARNING		
Stakeholder workshops and conferences Hard copy registration forms Hard copy evaluation forms Hard copy QA feedback	Shredded within month of event	Destroy under secure conditions
Electronic event folder Venue contracts Delegate contact details Delegate registration and attendance details Delegate certificates Event organisation correspondence (emails) QA feedback on adviser facilitators	6 years	Destroy under secure conditions
Training materials (including programme)	20 years	Return to archive
Press cuttings/ online media monitoring	1 year	Archive
Press Releases	7 years (5 years online)	Archive

Type /Subtype of Record	Minimum Retention Period	Action at end of retention period
Newsletters	7 years (5 years online)	Archive
Blogs and other social media	7 years (5 years online)	Archive
leaflets	7 years (5 years online)	Archive
Image library	10 years (5 years online)	Archive
Case studies (anonymised)	30 years (10 years online)	Archive
Root cause analysis	30 years	Archive
Thematic reviews	30 years (30 years online)	Archive
Event organisation correspondence (emails)	7 years (5 years online)	Archive
Blogs and other social media	7 years (5 years online)	Archive
leaflets	7 years (5 years online)	Archive
Image library	10 years (5 years online)	Archive
Case studies (anonymised)	30 years (10 years online)	Archive
INFORMATICS		
FOI Data Requests	6 years	Destroy under secure conditions
Member Data Requests	6 years	Destroy under secure conditions
Internal Data Requests	6 years	Destroy under secure conditions
FOI Data Responses	6 years	Destroy under secure conditions
Member Data Responses	6 years	Destroy under secure conditions
Internal Data Responses	6 years	Destroy under secure conditions
National Audit Office Data Requests	6 years	Destroy under secure conditions
National Audit Office Data Requests	6 years	Destroy under secure conditions
Parliamentary Questions Data Requests	6 years	Destroy under secure conditions
Parliamentary Questions Data Responses	6 years	Destroy under secure conditions
Annual Report Data	6 years	Destroy under secure conditions
Panel Data Requests	6 years	Destroy under secure conditions
Panel Data Responses	6 years	Destroy under secure conditions
Internal Audit Reports	Lifetime of the (organisation plus 6 years) 6 years	Archive
Business Plans	Lifetime of the (organisation plus 6 years) 6 years	Archive
Fact Sheets	Lifetime of the (organisation plus 6 years) 6 years	Archive
Claims Data Databases	75 years after case closure (Subject to preliminary guidance Project E.R.I.C)	Archive
Practitioner Performance Advice Service Referral Data Database	75 years after case closure (Subject to preliminary guidance Project E.R.I.C)	Archive