POLICY AND PROCEDURE: DATA RETENTION AND DESTRUCTION

NUMBER: 147

CARE FOR VETERANS POLICY

1 INTRODUCTION

1.1 The way in which data is recorded and maintained within any organisation is crucial to allow effective function. The way in which this data is controlled is essential for maintaining good working practices.

1.2 Without adequate maintenance of all forms of data, trust in any organisation to provide the highest standards of care will diminish and data may be retained unnecessarily.

1.3 The purpose of the Retention and Destruction Policy is:

- to provide all staff with a clear and precise framework from which to manage data
- to prevent unnecessary retention of data with the associated unnecessary use of storage space
- to ensure that Care for Veterans (CfV) conforms to current regulations
- to ensure compliance with our legal responsibilities.

1.4 The destruction of records is an irreversible act. The guidelines for the retention of both electronic and physical data is included in the departmental appendices.

- Relevant regulation must be considered before activating retention periods in this schedule.
- Decisions should be considered in view of the need to preserve data, the use of which cannot be anticipated fully now, but which may be of value to future generations.
- Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.
- The provision of the General Data Protection Regulation (GDPR) 2018 must be complied with.

- Permanent Preservation of records can be employed in the interest of scientific, statistical or historical reasons if there is a legitimate reason.

1.5 This Policy is issued and maintained by the Chief Executive (the sponsor) on behalf of Care for Veterans and supersedes and

replaces all previous versions.

2 POLICY STATEMENT

2.1 Care for Veterans Trustee Board acknowledges the importance of data and is committed to the creating, keeping, maintaining and disposing of all data, including electronic records, commensurate with legal, operational needs and in accordance with the GDPR.

2.2 A Data Protection Impact Assessment (DPIA) has been carried out and has concluded that this policy is of low-impact.

3 DEFINITIONS

In this Policy,

Data:	includes all records completed and held in respective of the CfV's business that contain data relating to both health and administration. Records include both paper and electronic records.
The PRA:	The Public Records Act (1958).
The PRO:	The Public Records Office
The Policy:	The Retention and Destruction of Records Policy

4 ROLE AND RESPONSIBILITIES

4.1 Statutory Responsibility

The Information Commissioner's (ICO) office and the Secretary of State for Health and all care delivery organisations have a duty under the PRA, to make all possible arrangements for the safe-keeping and eventual disposal of all types of data. The Chief Executive and senior managers are personally accountable for the destruction of records within their respective areas of operation.

4.2 Managerial Responsibility

4.2.1 The Trustee Board has a responsibility to ensure and gain assurance that CfV has in place robust arrangements for the destruction of data and that these arrangements are complied with.

4.2.2 The Chief Executive has responsibility to implement robust and appropriate record management arrangements in accordance with national and statutory requirements.

4.2.3 The Chief Executive delegates responsibility to senior managers for the management of data in their respective areas at CfV.

4.3 Individual Responsibility

All CfV staff are responsible for any data that they create or use. This responsibility is established and defined by GDPR and the law. Every CfV employee who processes, handles, stores or otherwise comes across data has a personal common law duty of confidence.

5 SCOPE OF POLICY

5.1 This policy relates to the retention and destruction (or permanent preservation) of all data including but not limited to:

- Accounting records and budgetary data;
- Board, committee and sub-committee meeting minutes;
- Contracts;
- Personal work diaries;
- Health records data (including NHS);
- Invoices;
- The contents of Personnel files;
- Payroll / PAYE records;
- Litigation dossiers, including complaints, claims and inquest files;
- Policy and procedure manuals;
- Software licences;

5.2 This policy covers the clinical areas, human resources, fundraising, support services and administration services including finance.

6 AIMS AND OBJECTIVES OF THE POLICY

Objectives

The main objectives of the Policy are to ensure:

6.1.2 **Accountability**

That records are maintained to account fully and transparently all actions and decisions, in particular:

- To protect legal and other rights of staff, residents or visitors;
- To facilitate audit or examination;
- To provide credible and authoritative evidence if required by law.

6.1.3 **Quality**

That all records are periodically, and routinely reviewed to determine which can be disposed of or destroyed. This will guarantee the quality of any data that is selected for permanent preservation.

6.1.4 **Accessibility**

That records which have been selected as archives will be held in a suitable area that will guarantee appropriate conditions for storage and access

6.1.5 **Training**

CfV staff are to be made aware of their responsibilities relating to the processing of data and advised where to find guidance about the retention and destruction of records on Induction and as part of their ongoing Mandatory training

6.1.6 **Security**

The destruction of confidential data ensures that confidentiality is maintained. Destruction is to be by cross-cut shredding or via a confidential bag system. It is the responsibility of CfV to satisfy itself that the methods used throughout all stages, including transportation to the destruction site, provides satisfactory safeguards against

accidental loss or disclosure. A certificate of destruction will be issued by the contractor.

6.1.7 **Performance Measurement**

The process of retention and destruction of records procedures are monitored and action taken to improve standards if necessary

6.1.8 **Notes on preservation of patient records for historical purposes**

6.1.9 For medical and historical research in cases of interest, it may be appropriate to select some records for permanent preservation. Selection should be performed in consultation with health professionals and archivists from an appropriate place of deposit. If records are to be sampled, specialist advice should be sought from the Worthing NHS Trust or NHS England about their storage. Explicit consent should be sought from the resident's next-of-kin.

6.2 All electronic and paper records that are selected for destruction must be recorded on the departments Destruction Log, an example of which can be found in Appendix 1.

7 EVIDENCE BASE

This policy has been developed with reference to:

- Department of Health – Records Management: NHS Code of Practice Parts 1 and 2
- NHS Litigation Authority Standards
- Care Quality Commission (CQC Standards)

8 MONITORING COMPLIANCE

8.1 The ICO, CQC and HMRC may monitor CfV's performance in respect of records, retention and destruction

8.2 The Trustee Board are responsible for monitoring compliance with the Policy

8.3 The Information Commissioner, who is the Supervising Authority for data, may perform assurance visits

9 TRAINING REQUIREMENTS

9.1 All staff must be appropriately trained so that they are fully aware of their responsibilities in respect of the retention and destruction of records.

9.2 Staff induction programmes will include training on the data protection including the retention and destruction of records.

9.3 Staff will undertake data protection as part of their mandatory annual training

9.4 Heads of Department will oversee their own departmental data and ensure that staff acting as processors do so in accordance with regulations.

10 DISTRIBUTION

The Policy, once approved, will be included within CfV's policy library

11 COMMUNICATION

All Managers will be informed of this Policy and will ensure staff are made aware of its content and location.

12 APPENDICES

APPENDIX 1 ***EXAMPLE***

Records Destruction Log

Description of Record to be Destroyed	Electronic / Paper	Department	Person Authorising	Retention Period	Date of Destruction	Nominated Person
Email account for Joe Bloggs	Electronic	Clinical	IT Manager	1 year after staff member has left	02.11.2018	Example
Minutes of Staff meeting	Paper	CEO	CEO	3 years	05.11.2018	Example

13 Clinical Department

Data	Minimum Retention Period (Years)	References /Notes
Resident's medical notes	Duration of resident's stay, then eight years after death or discharge.	Department of Health's Record Management Code of Practice for Health and Social Care 2016
CareSys.	Duration of resident's stay, then eight years after death or discharge.	Department of Health's Record Management Code of Practice for Health and Social Care 2016
MAR charts.	In use for one month then archived and kept for eight years.	Department of Health's Record Management Code of Practice for Health and Social Care 2016
Appointment data.	Duration of residents stay, then eight years after death or discharge.	Department of Health's Record Management Code of Practice for Health and Social Care 2016
Resident outing / social data.	Shredded at ward level after event. Copy kept for one year in Social and Rec and Quality Assurance.	Residents wish to have their names on public view as a reminder re events / outings etc.
Resident correspondence. (Personal mail)	Given to resident or placed in residents file.	Delivered to residents by senior staff daily, on receipt of same. Forwarded to ex-resident or NOK following discharge or death
Hand over sheets	One shift	Staff instructed to shred at end of shift. Kept in uniform pocket while o duty

Data	Minimum Retention Period (Years)	References /Notes
Staff rosters	On computer. Hard copy archived for eight years	CQC Guidance: GDPR Awareness for Care Homes Training Course
Training records	Seven years	1 CQC guidelines Regulation 19 2 Records Management Code of Practice for Health and Social Care 2016
IPR / Supervision.	Kept for duration of employment.	1 CQC guidelines Regulation 19 2 Records Management Code of Practice for Health and Social Care 2016
Annual Leave / Request books.	Four Years	1 CQC guidelines Regulation 19 2 Records Management Code of Practice for Health and Social Care 2016

14 Human Resources

Data	Minimum Retention Period (Years)	References /Notes
Application Forms – unsuccessful applicants	Six months	Chartered Institute of Personnel and Development – non-statutory recommended retention period due to possible discrimination claims.
Staff Records	Seven years then a summary to be kept until 75th birthday	1 CQC guidelines Regulation 19 2 Records Management Code of Practice for Health and Social Care 2016
Occupational Health Reports	Seven years	1 CQC guidelines Regulation 19 2 Records Management Code of Practice for Health and Social Care 2016

15 Fundraising

Data	Minimum Retention Period (Years)	References /Notes
Contact details of donors on Donorflex database	See note opposite	Once on the Donorflex database and financial data against the donor's details, cannot be deleted from the database. However, the donor can withdraw consent
Contact details of those on Donor Strategy	Three years	Donor Strategy database transferred to Donorflex database in 2018. Old details retained to allow code compatibility.
Gift Aid declarations, reports and claims	Until the donor ceases to donate	HMRC: Retention and disposal policy 4.1 HMRC retention policy
Credit/debit card details from payments received	Never retained	No details retained -shredded immediately after the payment has been processed.
Legacy data	Seven years	HMRC: Retention and disposal policy 4.1 HMRC retention policy

16 Support Services

Data	Minimum Retention Period (Years)	References /Notes
Rosters	Electronic copies kept on shared drive. Deleted after one year. Hard copies given directly to individual staff members	Compliance under GDPR
Signing in sheets – visitors	One month	Changed visitors signing in book to be compliant with GDPR
CCTV	21 days unless footage required for evidential purposes in legal proceedings	https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

17 Administration / Finance

Data	Minimum Retention Period (Years)	References /Notes
Accounting records including payroll	The default standard retention period for HMRC records is 6 years plus current, otherwise known as 6 years + 1. This is defined as 6 years after the last entry in a record followed by first review or destruction to be carried out in the additional current (+ 1) accounting year.	HMRC: Retention and disposal policy 4.1 HMRC retention policy https://www.gov.uk/government/publications/hmrc-records-management-and-retention-and-disposal-policy/records-management-and-retention-and-disposal-policy#retention-and-disposal-policy
Pension schemes - Defined Benefit Scheme - Work Place Pension Scheme	Minimum of six years.	The retention periods are requirements from the Pension Regulator https://www.thepensionsregulator.gov.uk/en/trustees/managing-db-benefits/governance-and-administration/record-keeping
Data Technology - Email Addresses	Email addresses for individual staff members (when name specific) are kept for a maximum of 30 days. Once deleted from Office 365 the data remains with Microsoft for a further 30 days from deletion in case recovery required. After this point the data is permanently deleted.	Email addresses do not contain any other personal/sensitive data other than the name of the employee. https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies
Contracts – less than £5000	Two years	http://nationalarchives.gov.uk/documents/data-management/sched_accounting.pdf
Contracts – greater than £5000	Records relating to contracts that are for a period of more than ten years should be reviewed when they are five years old to determine whether they are still needed for current business and thus for further retention. Thereafter they should be reviewed every five years.	http://nationalarchives.gov.uk/documents/data-management/sched_accounting.pdf

18 FURTHER GUIDANCE

Medico-legal Value of Archived Material
In general, for forensic purposes, (whether civil, criminal or coronial), documents consisting of original and contemporaneous medical data must be retained. The primary value of direct witness testimony on oath should not be forgotten. Courts are prepared to accept electronic data in civil cases and, provided additional safeguards are complied with, also in criminal cases. In criminal and civil cases, statements contained in documents which are received in evidence may be proven by copies of the original documents, provided that such copies are adequately authenticated. Thus, although original records are desirable, this must be balanced against the convenience and practicality of making copies or preserving them in computerised or microfiche form. However, as a matter of practice, it is necessary to maintain records of the fact of computerisation or of the copying process in relation to any documents to facilitate subsequent authentication and admissibility.
Teaching records
Selected photographs, medial data and other relevant data, can be a resource for teaching purposes. These should be logged, adequately indexed, described and catalogued, in the archives or in local, central or national archives.

Research data and audit
Confidential named patient data (documentation) collected during an investigation or audit and held separately from the patient's records should be destroyed or anonymised six months after the research/audit has been completed, the data analysed and final publication of the finding has been made. If further recourse to named data is anticipated, it may be kept indefinitely. Working records and other research data should be retained permanently to rebut allegations of scientific fraud if such are made. Records and clinical trial data on medicines must be kept for 15 years (Good Clinical Practice). The provisions of the General Data Protection Regulations 2018 must be observed for these as for other pathological records.

Confidentiality of Records
Health Care Professionals carry the prime responsibility for the protection of data given to them by their patients or obtained in confidence about patients. They must therefore take all steps to ensure that, as far as lies within their control, the records, manual and computerised, which they keep or have access to or which they transmit are protected by effective security systems with adequate procedures to prevent improper disclosure. Medical data portability is acceptable under GDPR but the primary responsibility lies with the sender and key step is to establish that the receiving terminal is in a 'safe haven' The provisions of COSHH regulations and of Health and Safety at Work legislation must be observed.
Long term (permanent) retention of records

Retention of data beyond 30 years, other than in the case of regional historical or teaching or research archives already kept in places of deposit, (which may include the premises of medical institutions), requires an application to the Lord Chancellor through the Keeper of Public Records if there is a need for them to be retained by the Charity or local Health Authority, rather than be transferred to a place of deposit or be destroyed.