Policy and Procedure on Record Management

Policy Author / Reviewer	Nicholas Foster
Approval Date	September 2020
Next Review Date	September 2022
Version No	1
Policy Level	Group
Staff Groups Affected	All Staff

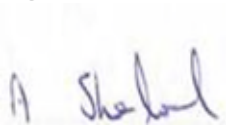
Contents

1. **Terminology** 2
2. **Introduction** 3
3. **Purpose** 3
4. **Policy** 3
5. **Accountability / Responsibilities** 4
6. **Procedures** 4
   - Data Protection 4
   - Record creation 4
   - Record Keeping 4
   - Record Security 5
   - Record Maintenance 5
   - Disclosure and Transfer of records 6
   - Record Closure 6
   - Retention of records 6
   - Disposal of records 6
   - Retrieval of records from archives 7
7. **Standard Forms, Procedures and Relevant Documents** 7

Monitoring and Review

The Proprietor will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than two years from the date of approval shown above, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed:



Amanda Sherlock
Senior Information Risk Owner (SIRO)
Director, Compliance & Regulation
October 2020

1. Terminology

1.1. Our aim is to use consistent terminology throughout this policy and all supporting documentation as follows:

Records	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. This is any information, regardless of format or medium, captured in a reproducible format.
Records Management	Creation, maintenance, control, storage and disposal of records in a way which facilitates their most appropriate, efficient and effective use.
Document	A document is any piece of written information in any form, produced or received by an organisation or person. Note all records start off as documents, but not all documents will ultimately become records.
Disposal	The decision as to whether the record should be destroyed, transferred to an archives service for permanent preservation or presented and the putting into effect of that decision.
'Establishment' or 'Location	this is a generic term which means the service users' home/school/college
Individual	means the service user
Service Head / Head of Service / Locality Manager	This is the senior person with overall responsibility for the Location.
Key Worker	Members of staff that have special responsibility for Individuals residing at or attending the Establishment.
Parent, Carer, Guardian	means parent or person with Parental Responsibility or Powers of Attorney for the service user
Regulatory Authority	Regulatory Authority is the generic term used in this policy to describe the independent regulatory body responsible for inspecting and regulating services.
Social Worker	This means the worker allocated to the child/family. If there is no allocated worker, the Duty Social Worker or Team Manager is responsible.
Placing Authority	Placing Authority means the local authority/agency responsible for placing the child or commissioning the service
Staff	Means full or part-time employees of CareTech, agency workers, bank workers, contract workers and volunteers.

2. Introduction

2.1. This document sets out the procedures which cover treatment of all types of records within CareTech Holdings Plc ("CareTech"). It is intended to provide practical guidance relating to the creation, storage, access to and destruction of records.

2.2. This policy has been approved by and applies to CareTech and its direct and indirect subsidiaries and references to the "CareTech" shall be construed as referring to all such companies.

2.3. Its affects all staff. Everyone must make sure that they are familiar with the detail and what is expected of them under the policy.

3. Purpose

3.1. The purpose of this document is to ensure that our record management practice meets all operational, legal and regulatory requirements.

3.2. Specifically, the purpose of these procedures is to provide methods whereby CareTech can meet the provisions and requirements of the General Data Protection Regulations, the Data Protection Act (2018) and the recommendations of the Caldicott Committee.

3.3. The aims of this document are:-

- To establish a set of procedures relating to the creation, use, storage, management and disposal of all types of record
- To clarify the legal obligations relating to records held by CareTech
- To set out the minimum periods for retention of different types of records
- To co-ordinate the resulting maintenance, disposal or preservation of records.

4. Policy

4.1. The guidelines in this document cover all types of records regardless of the media on which they are held. As new media appear these should be added to this list.

4.2. They may consist of:-

- Electronic or paper Service User health/education records
- Administrative records
- Photographs, slides and other images
- Microfilm / microfiche
- Audio and video tapes, CDs, DVDs and other media
- Emails
- Computerised records
- Scanned records
- Text messages.

5. Accountability / Responsibilities

5.1. The Information Governance Board is responsible for the review and development of this and other information governance policy documents.

5.2. Heads of Establishment are responsible for ensuring that their staff have read and understood these procedures and have been provided with adequate training to carry the procedures out effectively.

5.3. All employees must understand their responsibilities in respect of records management and ensure that the procedures in this document are adhered to.

6. Procedures

Data Protection

6.1. Heads of Establishment and function managers must ensure that records containing personal data are:-

- Obtained in keeping with the Data Protection Policy
- Not used for other purposes for which the information was not originally obtained
- Kept for no longer that necessary for the specified purpose (see below – Retention Periods)
- Adequate, relevant, accurate, proportionate to the purpose and kept up to date
- Handled in accordance with the person's rights under the Data Protection Act
- Safeguarded against unauthorised access or use, loss or damage
- Not transferred to another country without first seeking approval from the Group's Data Protection Officer
- Destroyed by an appropriate method when no longer required.

6.2. They must also ensure that Service Users are allowed to access records and information about them and provided with assistance in the maintenance of these records, where appropriate.

Record creation

6.3. Records must be complete and accurate to ensure the quality of services provided by CareTech. Where possible, records are to be completed in the presence of, and with the co-operation of the individual.

6.4. All records, case notes, documents and personal information should be signed and dated appropriately by the person creating or updating the records.

6.5 To ensure that the record is reliable it is important that the details of the author, the subject and the date it was created are recorded on the document. If it is a draft version, it should be marked accordingly. If there are multiple drafts and a final version held on a file, clear and consistent version control should be used (Version 1, 2, 3 etc.).

Record Keeping

6.6. Records (paper and electronic) should be arranged in a structured filing system which allows rapid, efficient and reliable retrieval of information.

6.7. All record systems must include a documented set of rules for referencing, titling, indexing and referencing information and should be stored with due regard to information security and confidentiality requirements.

6.8. Employees must ensure that records are kept and maintained in accordance with the record keeping system.

6.9. Electronic records should only be stored in authorised locations (e.g. electronic Share Folders or within an electronic document management system) to ensure that they are backed up by CareTech's central backup systems. This will ensure that information cannot be lost or corrupted by a technical breakdown. As a general rule, records should not

be stored on personal devices (mobile phones or iPads) or on the local hard drive of any desktop PC, laptop or any portable media solution (USB or disc) which is not subject to a routine backup strategy.

6.10 For offline records, staff should ensure their computer hard disk is encrypted. Encryption equally applies to removable media e.g. memory sticks, DVDs and external hard disks.

6.11. Employees must ensure that they understand where records relevant to their job are stored and how they must access them.

Record Security

6.12. All manual files or documents of a confidential nature must be stored securely in a lockable filing cabinet with higher levels of security for records containing sensitive personal data. All the keys must be stored in a secure key box and staff should lock records away when absent for extended periods e.g. overnight.

6.13. Records should only be accessed by employees who have a need and a right to access them.

6.14. No files or documents of a confidential nature should be left out where they can be read by unauthorised employees or others (please refer to the Clear Desk Policy).

6.15. Employees should ensure that they do not provide unnecessary access to records to others. More specifically they should:-

- Use passwords on systems and documents where appropriate and never divulge passwords to others except where this is necessary to effect formal transfer of information (e.g. in the case of a password protected document or file).
- Log off systems (or otherwise make them inaccessible to others) when leaving the computer even for a short period
- Never leave a computer with Service User or other confidential information on screen and actively ensure that confidential information cannot be overseen.

6.16. Laptops, tablets and smart phones containing records must have tracking mechanism and, in case of theft or loss, and a facility to remotely lock the laptop, and if necessary, remotely wipe the date.

6.17. Staff must not take records off site without prior written authorisation of their line Manager. If authorised, staff member taking records off site must not leave their laptop, other devices or any hard copies of records in public places. A log of records must be kept showing what records are off site and who is holding them.

Record Maintenance

6.18. The location and movement of records must be controlled to ensure that records may be retrieved at any time, that any outstanding issues can be dealt with and that there is an auditable recorded trail of transactions and changes to records. Storage locations must be kept orderly and tidy and should prevent damage to records

6.19. Employees should perform regular checks on the accuracy of records and inform their line manager if errors are identified.

6.20. Regular checks must also be carried out to remove any personal data or records that are no longer relevant or out of date. Every effort must be made to ensure the accuracy of personal data collected allowing for the personal data to be amended, removed or clarified where appropriate.

Disclosure and Transfer of records

6.21. Procedures covering the disclosure and transfer of records are set out in the Confidentiality Policy. In general, no confidential data should be released to anyone who is not specifically and explicitly authorised to do so, and such information should only be disclosed after explicit permission has been given by the Group's Data Protection Officer or Caldicott Guardian. A record of the data disclosed should be made.

6.22. Staff must password protect or encrypt records before emailing them. Furthermore, staff must double check their emails TO and CC recipients before emailing records. Staff should:

- Change their passwords regularly.
- Not share their passwords with others unless there is a justified business need and authorisation.
- Ensure their passwords are strong.

Record Closure

6.23. Paper records should be closed and transferred to secondary storage locations once they have ceased to be of use for current care, clinical, residential, fostering, educational or commercial purposes. This closure should be noted on the records and an inventory maintained showing from where information may be retrieved should it become required.

Retention of records

6.24. Records should be retained where there is a legal duty to keep them or to fulfil a business need and for as long as is necessary for the purpose which they were originally collected. The records should be archived and retained for at least the period set out in the table in Retention Schedule for the respective service area.

6.25. When archiving record, each location must follow the procedure which is outlined on **Appendix 1 – Archiving Procedure.**

Disposal of records

6.26. Records can then be destroyed once they reach the end of the respective retention period. The method of destruction should match the sensitivity of personal data being destroyed. Electronic records should also be deleted from systems however where this is not technically possible, they should be 'put beyond use'.

6.27. Heads of Establishment are responsible for ensuring a review of records is conducted at least every six month to ensure that they are archived and disposed of in accordance with the relevant retention period.

6.28. Records should be disposed of in an appropriate and secure manner. Where hard copy records are to be destroyed, the Head of Establishment or function manager should ensure that it is undertaken in a way consistent with the sensitivity of the information. This may include shredding, incineration or by an approved secure disposal service. Under no circumstances should any records be placed in the general waste collection service.

6.29. For digital information, employees should make use of authorised destruction services for media such as hard disk drives, CDs, DVDs and tapes.

6.30. Records of the destruction of records should be kept setting out the records destroyed, the manner of destruction, the date of destruction and any confirmatory documentation received from the party responsible for the physical destruction of the records. This document should be sent to data.protection@caretech-uk.com so that the central database can be updated accordingly.

Retrieval of records from archives

6.31. Heads of Establishment are responsible for ensuring that a record inventory is maintained for all archived records to facilitate quick and easy retrieval (see **Appendix 2 – Record Inventory**). Records sent to Restore Document Management can be retrieved via Restore Web by entering the relevant barcode. The Head of Establishment or function manager is responsible for ensuring that records are returned to archives.

7. Standard Forms, Procedures and Relevant Documents

7.1. Appendix 1 - Archiving Procedure

7.2 Appendix 2 – Record Inventory