
RECORD KEEPING POLICY

Effective Date:	28/09/2010	Approved by:	Graham Oakes
Review Period:	Biennial	Affecting:	All staff

Links embedded in the text of this e-policy are intended to facilitate the location of related policies, procedures and forms, and give access to external websites offering more detailed information.

PLEASE REPORT ANY ERRORS IN THIS POLICY

Aim

The aim of this policy is to inform our staff of the way in which data should be obtained, recorded, stored and accessed in accordance with the [Data Protection Act 1998](#)

Policy

Definitions

Client

Where in this policy we have referred to “client” or “clients”, the term refers to either Care at Home Clients or Care Home Residents as appropriate.

Background

Any one who obtains personal information (“data”) about other individuals is a *Data Controller* and is thus regulated by the [Data Protection Act 1998](#).

The Act controls what can lawfully be done with information. It also gives people certain rights to control how information about them is obtained, used, stored and distributed. These rights include the right to find out what information a *Data Controller* has about them, and ask for copies of that data.

We obtain information about our staff and clients as part of our function and have nominated *Data Controller* individuals for each care home and office.

Compliance with the Data Protection Act 1998

Altogether Care LLP and its two subsidiary companies, *Altogether Care – Care Homes Ltd* and *Altogether Care - Care at Home Ltd*, are registered under the [Data Protection Act 1998](#) (the Act) and all storage and processing of personal data held in manual records and on computers in the three companies should comply with the Act.

We understand that, according to the Act, all personal data should:

- be obtained fairly and lawfully
- be held for specified and lawful purposes
- be processed in accordance with the person's rights under the Act

- be adequate, relevant and not excessive in relation to that purpose
- be kept accurate and up to date
- not be kept for longer than is necessary for its given purpose
- be subject to appropriate safeguards against unauthorised use, loss or damage
- be transferred outside the European Economic Area only if the recipient country has adequate data protection.

Data Controllers

Under the Act, we must nominate a Data User/Data Controller, therefore:

- The *Data Controller* for each care home and Care at Home office is the *Registered Manager*, who may delegate the tasks associated with the practical aspects of data control to others, but retains the overall responsibility for the security and storage of the data controlled by their office or care home.
- The *Data Controller* for our Head Office is the *Head of Administration*, who may delegate the maintenance tasks as appropriate, and also some of the responsibility to other management level staff as necessary and appropriate. Such delegation of responsibility should be confirmed by both parties in writing (emails acceptable)

Types of record, record handling and storage times

The table below lists the different kinds of controlled data and for how long they should be stored in compliance with the Act and also with *Outcome 21* of the Care Quality Commission's *Essential Standards*:

Data type	Storage time
Client Plans / Plans of Care	8 years
Risk Assessments	Retain the latest risk assessment until a new one replaces it
Interview/recruitment records for unsuccessful applicants	6 months
Purchasing (excluding medical devices and equipment)	18 months
Incidents, occurrences and events requiring notification to CQC	3 years
Use of restraint or the deprivation of liberty	3 years
Maintenance of the premises	3 years
Maintenance of equipment	3 years
Electrical testing	3 years
Fire Safety	3 years
Water safety	3 years
Medical gas safety, storage and transport	3 years
Money or valuables deposited for safe keeping	3 years
Staff employment	3 years following date of last entry

Duty rosters	4 years after the year to which they relate
Purchasing of medical devices and medical equipment	11 years
Final annual accounts	30 years

We believe the following rules should apply to all *Data Controllers*, and to any members of staff who are handling data on their behalf:

- Individual records and home records should be kept in a secure fashion, up to date and in good order; and are constructed, maintained and used in accordance with the Act, ISO 9001(2009) and *Outcome 21* of the CQC *Essential Standards*.
- Records required for the protection of clients and for the effective and efficient running of our business;
 - are to be kept at the business premises and should not be taken from the premises without the express permission of the person whom the data concerns, and the *Data Controller* (this includes data stored on laptops, memory sticks and the transmission of data via the internet and emails where these are not adequately protected by passwords and encryption)

PLEASE NOTE: If electronic monitoring systems are in use, the password to access the data on the mobile device should never be given to anyone who does not need to know it, or written down in any format among the device user's possessions (for example it should never be noted on a piece of paper in the user's pocket)

- should be regularly updated and accurate,
- should remain confidential to the staff involved and the individual about whom the data is stored,
- should never be distributed prior to the consent of the owner (the person to whom it relates)

PLEASE NOTE: the wilful failure of any member of staff, to whom the responsibility for carrying out the task of maintaining the records has been delegated, will be treated as a disciplinary offence.

Access to Records

Clients and members of staff should have access to their records and all the information held about them, as well as opportunities to help maintain their personal records.

Any client requiring access to their office kept files should contact the Registered Manager to make arrangements to view them. Clients with sensory impairment or other disabilities must be given appropriate help and support from an independent source as required.

The viewing of certain records may only be refused under the following circumstances as consistent with the Act:

- where disclosing the personal data would reveal information which relates to and identifies another person unless that person has consented to the disclosure or it is reasonable to comply with the request without that consent
- where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person

- where the request for access is made by another on behalf of the data subject, access can be refused if the data subject had either provided the information in the expectation it would not be disclosed to the applicant or had indicated it should not be so disclosed, or if the data was obtained as a result of any examination or investigation to which the data subject consented on the basis that information would not be so disclosed.

Before deciding whether the above restrictions apply, the *Data Controller* should consult the health professional responsible for the clinical care of the client or resident, or if there is more than one, the most suitable available health professional. If there are none then the *Data Controller* should consult a health professional with the necessary qualifications and experience to advise on the matters to which the information requested relates.

Clients who have a complaint about the way that the organisation keeps files about them, or who are refused access to files that they believe they should have access to, should be referred to the [Information Commissioner's Office](#).

Procedure

General data protection procedure

1. Staff should do the following:
 - a. Ensure that all files or written information of a confidential nature are stored in a secure manner in a locked filing cabinet and are only accessed by staff members who have a need and a right to access them to fulfil the duties of their role, and that this information is never left out where it can be read by others.
 - b. Wherever practical fill in all care records and client notes in the presence of and with the co-operation of the client.
 - c. Ensure that all care records and client notes, including Plans of Care and Client Plans, are signed and dated.
 - d. Check regularly on the accuracy of data being entered into computers.
 - e. Always use provided passwords to access the computer system and do not abuse them by passing them on to people who had not been authorised to use the system for the password permitted purpose.
 - f. Use computer screen blanking to ensure that personal data is not left on screen when not in use. (press the *Sleep* button on your keyboard, or CTRL ALT DEL and then click *Lock Computer*)

Controlled data kept in the homes of our Care at Home clients' Client Files

2. With the client's consent, the care or support workers should record, in records kept in the home of client, the following information:
 - a. the time and date of every visit to the home
 - b. the service provided
 - c. any significant occurrence.
3. Where appropriate, records should include:
 - a. care given.
 - b. assistance with medication — including time and dosage

- c. financial transactions undertaken on behalf of the client
 - d. details of any changes in the client's or carer's circumstances, health, physical condition or care needs
 - e. any accident, however minor, to the client and/or care or support worker
 - f. any other untoward incidents
 - g. any other information that would assist the next health or social care worker to ensure consistency in the provision of care.
4. Records should be kept in the home for one month, or until the service is concluded, after which time they should be transferred, with the permission of the client, to the Care at Home office or other suitable body (eg local authority or health trust, or other purchaser of the service), for safe keeping in accordance with the time limits set by the Care Quality Commission Essential Standards, Outcome 21, and set out in the table below.

PLEASE NOTE: staff should ensure that all care records and notes, including Client Plans and Plans of Care, are signed and dated by the relevant parties

Procedure for confirming the existence and maintenance of records

5. The Registered Manager is to muster and personally check the existence, maintenance and completeness of all records listed above each month. Any errors or omissions found are to be investigated by the Registered Manager and action taken to rectify them. The registered provider places special emphasis on good record keeping.

Photography

6. There may be occasions in which the use of photography may assist in the delivery of client care, eg for drug charts. The taking of photographs is only to be done with the express written permission of the client or resident using the appropriate *Photography Permission Form* and is only to be used for the explicit purposes of delivering care after the *Photography Release Form* has been completed and signed.
7. Photographs taken for this purpose are to be treated in the same way as other documentation relating to client care and given the same security arrangements.
8. All photographic records whether on mobile phone, digital or conventional camera plus any resulting negatives are to be destroyed once the photographs have been printed.
9. Keeping photographs on cameras or mobile phones after photographs have been printed or using the photographs for any purpose other than the care of the client or residence may be a disciplinary offence.

Training

All new staff should be encouraged to read this *Record Keeping Policy* as part of their induction process. Existing staff will be offered training covering basic information about confidentiality, data protection and access to records.

Training in the correct method for entering information in clients and residents records should be given to all care staff.

The nominated data user/data controller for the organisation should be trained appropriately in the Data Protection Act 1998.

All staff who need to use the computer system should be thoroughly trained in its correct use.

Applicable legislation

Outcome 21 of the Care Quality Commission Essential Standards which is based on Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010, and which may be summarised as follows:

People who use services can be confident that their personal records including medical records are accurate, fit for purpose, held securely and remain confidential [and] other records required to be kept to protect their safety and wellbeing are maintained and held securely where required.

This is because providers who comply with the regulations will: keep accurate personalised care, treatment and support records secure and confidential for each person who uses the service; keep those records for the correct amount of time; keep any other records the Care Quality Commission asks them to in relation to the management of the regulated activity; store records in a secure, accessible way that allows them to be located quickly [and] securely destroy records taking into account any relevant retention schedules.

References

The NHS Constitution (Department of Health, 2009)

Records management: NHS code of practice (Department of Health, 2006)

Guidelines for Records and Record Keeping (Nursing and Midwifery Council)