

## **POLICY & GUIDANCE FOR THE MANAGEMENT OF RECORDS AND INFORMATION**

### **1. POLICY**

DRH accepts that a systematic and planned approach to the management of records and information within the organisation, from the moment that they are created to their ultimate disposal, ensures that the quality, quantity and confidentiality of the information that it generates is maintained. Information must be stored to standards which meet legal and regulatory compliance as well as professional practice recommendations.

**This Policy has taken into account the following:**

- Data Protection Act 1998
- Report on the Review of Patient Identifiable Information. DoH 1997
- Records Management: NHS Code of Practice
- Guidelines for Records & Records Keeping. NMC. 2005

### **2. WHAT IS A DRH RECORD**

In the context of this guidance a record is anything which contains information, in any media, which has been created or gathered as a result of any aspect of the work of staff employed by DRH.

### **3. THE PURPOSE OF SERVICE USERS & ASSOCIATED RECORDS**

Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence based Healthcare & social support. Information has most value when it is accurate, up to date and accessible when it is needed. An effective records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required.

The purpose of records created and maintained by DRH staff is to:

- Provide accurate, current, comprehensive and concise information concerning the support and care required by the service user .
- Provide a record of any problems that arise and the action taken in response to them
- Provide evidence of care and support required, details of interventions by nursing & support staff and service users responses.
- Provide evidence of the service users preferences and their ability to make choices.
- Provide continuity of care

- Document barriers to service users preferences and the actions necessary to overcome these barriers.
- Include a record of any physical, psychological or social factors that may affect the service user's well-being.
- Record the chronology of events and the reasons for any decisions made
- Support standard setting, quality assessment and audit
- Provide a baseline record against which improvement or deterioration may be judged.
- Support day-to-day business which underpins the delivery of care
- meet legal requirements, including requests from patients under subject access provisions of the Data Protection Act or the Freedom of Information Act;
- Support evidenced-based practice

#### **4. COMPLETION OF SERVICE USERS RECORDS**

All service user records kept within DRH should be easily legible to others, clear and unambiguous, signed, timed and dated on each entry. Any alterations or additions made are recorded in such a way that the original entry can still be seen. Amendments must also be signed, timed and dated.

#### **5. USING SERVICE USERS IDENTIFIABLE INFORMATION**

##### **Key Points:**

- DRH has a duty of care, by law, to keep service users information confidential
- Any unauthorised disclosure or misuse of service user's identifiable information constitutes a serious breach of discipline.
- A service user's identifiable information should never be left in a position where an unauthorised person can have access.
- Caution should be exercised when handling such information whether in written form, facsimile, computer screen, electronic or any other format.
- Access to all service users' identifiable information should be on a "need to know basis" and discussed only in the course of work.
- The overall responsibility for security of service users records lies with the Home Manager

***It is the responsibility of all members of staff to ensure that this policy and procedure is adhered to.***

#### **6. WHAT IS IDENTIFIABLE INFORMATION**

Identifiable information can be any information about any individual whether a member of the public, service user or staff. It can include:

- Name
- Address
- Postcode
- Telephone Number
- Date of Birth
- Occupation
- Religious beliefs
- Ethnic group

- Clinical details relating to disability, diagnosis, intervention and care
- An expression of opinion/experience surrounding the service user which may lead to their identification

## **7. GENERAL PRINCIPLES**

- Service user's identifiable information will only be handled by staff who are authorised to handle it as part of their duties
- Service user's identifiable information will never, under any circumstances, be communicated to persons who are not authorised to receive it.
- Access to all service users identifiable information, including individual records, is on a need to know basis.
- Service user's identifiable information will only be discussed with persons who need to know it in order to carry out their work.
- Whenever someone unknown to staff and not carrying an appropriate identification attempts to access service users identifiable information, they should be challenged and their proof of identity and authority sought.
- All staff should follow their professional codes of conduct .

## **8. PROCESSING SERVICE USERS IDENTIFIABLE INFORMATION**

Service user's identifiable information may be used and presented in a variety of ways including:

### **Verbal information/Telephones:**

- Any discussion of a service user must take place only with appropriate staff present, and in a location where the discussion cannot be overheard
- When dealing with requests for confidential information over the phone, it is essential that the identity of the caller is confirmed before a decision is made as to the appropriateness of disclosing information to them.
- If there is any doubt as to the identity of the individual, staff should 'phone them back to verify their identity, using a phone number obtained from an independent source.
- All staff should be cautious when giving out or confirming service user's identifiable information to a caller. It is recommended that staff be proactive in challenging the callers request and their genuine need for it.
- Where confirmation of service user's details is necessary in an area where they may be overheard, staff should ask the caller to repeat the details to them.
- All enquiries from the media concerning individuals must be dealt with by the Chairman, the Chief Executive or the Deputy Chief Executive.

### **Faxes:**

- All unsupervised fax machines that can receive service user's information must be located in an area that is secure so that unauthorised staff, or the general public, cannot gain access to them.
- Confidential information should only be sent by fax where absolutely necessary and then only if it is understood that the recipient is able to maintain security.
- If it is essential to fax confidential information a cover sheet containing a statement saying "this fact is confidential and is intended for the named person only" with a request that the recipient acknowledges safe receipt

- When faxing service users information measures must be taken to minimise the risk of mis-dialling. The safest method is pre-programmed dialling. Staff should avoid dialling from memory

### **Electronic Mail/Text messaging:**

- Confidential information should only be sent by email or text messaging when the sender is confident that confidentiality of the information will be maintained.
- If it is essential to email confidential information, a footnote signature containing a statement that "this information is confidential and is intended for the named person only" with a request that the recipient acknowledges safe receipt

### **Photocopying/Printers**

- Staff undertaking photocopying must ensure the return of the original document to the record. The copy must be afforded the same level of confidentiality and security as the original.
- Printing of service users identifiable information should not be undertaken on printers that unauthorised persons have access.
- Computer printouts containing service users information should either be filed securely or shredded as soon as they have been finished with.

### **Electronic Information**

- The same principles that apply to manual records also apply to electronic information. Confidentiality of any information held on computers hard drives, computer discs, memory sticks or mobile 'phones must be safeguarded.

### **Access to Confidential Records**

The records pertaining to service users are confidential. Relatives, friends and other visitors are not entitled to access them unless:

- Authorised to do so in writing by the service user
- They are a person appointed by a court of law to manage the affairs of a service user who is deemed incapable.

Information pertaining to service users may be shared in discussion with relatives and others directly involved in the individual's support providing any verbal disclosure is clearly in the best interests of the service user.

Persons seeking access to records must be challenged and their identity and authority to access the records confirmed.

**Procedures should be in place to ensure that work areas can demonstrate the maintenance of confidentiality. These procedures should be reviewed regularly**

## **9. RESPONSIBILITY FOR THE SECURITY OF RECORDS**

- Responsibility for ensuring the security and confidentiality of records including identifiable information concerning service users and staff within DRH homes lies with the appropriate Home Manager
- Responsibility for ensuring the security and confidentiality of identifiable records held in DRH offices lie with:
- The Chief Executive, the Deputy Chief Executive or the Company Accountant as appropriate.
- Records being transported between Homes by staff are the responsibility of the staff member concerned.
- Any member of staff transporting identifiable records must be authorised to do so. If records have to be taken overnight by a member of staff, they must ensure that they are safely stored within the house, and not left in a vehicle. Paper records should be transported in sealed envelopes or sealed bags and marked "confidential"
- Care should be exercised to ensure that memory sticks or discs are safely secured during transportation.
- If records have to accompany service users in ambulances or to clinics they must be in a sealed envelope and labelled.

## **10. STAFF AUTHORISED TO CARRY RECORDS BETWEEN HOMES**

- Support staff authorised by the Home Manager
- Head office staff authorised by the Chief Executive, Deputy Chief Executive or Company Accountant

## **11. THE PROTECTION AND USE OF SERVICE USERS INFORMATION**

### **Basic Principle**

Any information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without consent of the provider of the information. This is usually the service user, but sometimes another person (e.g. a fellow professional) may be the source.

The duty of confidence is long established as common law, but with proper safeguards, need not be construed so rigidly that, when applied, there is a risk of its operating to a service user's disadvantage. The best interests of the service user should always take priority.

Any prior request by a service user not to disclose certain kinds of information should normally be observed.

## **12. WHEN INFORMATION MAY BE PASSED ON**

In summary, information may be passed to someone else:

- With the service users consent **or** on a 'need to know' basis if the following apply:
  - The recipient needs the information because they are concerned with or involved in the service users care
  - Assuring and improving the quality of care and treatment
  - Monitoring and protecting public health
  - Co-ordinating care with other agencies, i.e. Local authority, NHS, etc.
  - Effective administration
  - Risk Management

- Statistical analysis or research
  - Statute or court order requires the information
  - Passing on information can be justified for other reasons (protection of the public)
- Staff not involved in the care of the service user either directly or indirectly, have no immediate right of access.
  - Police do not have an automatic right of access to confidential information. If in doubt seek advice from the Chief Executive or Deputy Chief Executive.

### **13. RESPONSIBILITY FOR PASSING ON INFORMATION**

Decisions to pass on information should be taken by the

- Home Manager responsible for the care of the service user.
- The Company Accountant for financial information
- The Chief Executive and Deputy Chief Executive for organisational matters

*If in doubt, seek the advice of the Chief Executive or Deputy Chief Executive*

### **14. SHARING INFORMATION WITH THE SERVICE USER**

It is DRH policy that any information recorded on a service user will be explained to them whenever practicable. All service users have the right to view their records if they wish. DRH recognise that good practice promotes maximum practicable involvement of the service user in the planning and implementation of their support. Records should always be written with a recognition of the service users right to inspect them. Records should always be respectful service user.

Full explanations must always given to the service user when it is proposed to pass on any health information when the referral is not from the service users GP or dentist. Full discussion should take place with the service user to obtain his/her agreement and consent.

### **15. PASSING ON INFORMATION TO RELATIVES, FRIENDS AND CARERS**

Requests for clinical or financial information from relatives should only be met following authorisation from the service user – unless the relative (or other advocate) has legal authority to obtain this information without the service user's express consent. Staff should always involve the service user and the person who has written the record.

This type of request should not be dealt with over the telephone but either in writing with reasons or in person.

### **16. STAFF PERSONAL RECORDS**

Personnel files are kept in secure cabinets locate at the place of employment. Home Manager records are retained at Connaught House. Additional staff files relating to salary payments and bank details are also held in secure files in the finance department. Except for statutory purposes (Care Quality Commission Inspections) information concerning staff will not be released to any third party without the written consent of the individual concerned. This includes information such as personal addresses and telephone numbers.

Requests for information should not be dealt with over the telephone, but either in writing with reasons or in person with means of identification and then only with the written consent of the member of staff concerned. No employee should disclose confidential information about a colleague without their expressed permission.

Any sensitive and identifiable electronic data held regarding staff should be securely stored. Information on hard drives should be password protected so that only the appropriate managerial staff have access. Memory sticks must be kept in secure conditions (e.g. on the owners person) when not in use. Care must be taken not to leave discs or memory sticks containing confidential information lying on office desks (etc) where they may be accessible to unauthorised persons..

Further relative information can be found in the Confidentiality Policy and Guidelines.

## MANAGING THE RETENTION AND DISPOSAL OF RECORDS

It is not possible to retain every record that is made and disposal is inevitable due to the high cost of storage and retrieval. However, the destruction of records is an irreversible act, and should always be carried out with care.

Most records, even administrative ones, contain sensitive or confidential information. **It is therefore vital that confidentiality is safeguarded at every stage** and the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding or incineration. It is the responsibility of the appropriate manager to ensure that methods used throughout the process provide adequate safeguards against accidental loss or disclosure of their contents. It is recommended that a brief description is kept of records that have been destroyed.

The decision to destroy records is the responsibility of the Home Manager or the appropriate Head of Department. If in doubt the Chief Executive, the Deputy Chief Executive or the Company Accountant should be approached for advice.

The length of retention periods for records depends upon the importance of the record and the following table is for guidance on **minimum** periods that records should be retained:

TYPE OF RECORD	RETENTION PERIOD	NOTES
Accident/Incident Forms & RIDDOR Reports	8 Years	From the date of the accident/incident. If litigation is involved, 8 years from the Date of settlement
Accident Registers	8 Years	
Annual Accounts (Final)	Permanent	
Accounts - Cost	6 Years	
Accounts – Working papers	3 Years	
Accounts – Minor records (pass Books, paying in slips, cheques, (other than cheques bearing printed receipts)accounts of petty cash expenditure, travelling and subsistence accounts, minor vouchers, duplicate receipt books, income records,	2 Years	From completion of the audit
Admission & Discharge Registers	8 Years	
Audit Records/original documents	2 Years	From completion of the audit
Audit Reports (including Associated records)	2 Years	After formal clearance
Bank Statements	2 Years	From completion of audit
Bills, receipts and cleared cheques	6 Years	
Budgets	2 Years	From completion of audit

<b>TYPE OF RECORD</b>		
Buildings & engineering works Town & country planning matters Agreements, conditions of contract, specifications, records drawings		Preserved for the life of the buildings and The installations to which they refer
Cash Books & cash sheets	6 Years	
Complaints	8 Years	From the settlement of the complaint or if Litigation is involved 8 years from the Date of completion
Creditor Payments	3 Years	
Death Records/registers		Permanent record
Debtors records/cleared	3 Years	From completion of the audit
Debtors records uncleared	3Years	
Diaries	3 Years	For Home diaries but general diaries can be Disposed of on completion.
<b>Establishment records: major</b> Personal files, letters of appoint- ment, contracts, references & related correspondence	3 Years	Keep for 6 years after person leaves or until 70th birthday whichever is the later.
<b>Establishment records: minor</b> Attendance books, annual leave Records, duty rosters, timesheets	2 Years	
Expense Claims	2 Years	From completion of audit
Forms – Pension(copies)	Permanent	Original sent to Pension Company
Funding data	6 Years	
Service user's records	8 Years	After discharge and then only after consultation with other health professionals involved in their care
Mentally Disordered persons (within the meaning of the Mental Health Act 1983)	20 Years 8 Years	After no further treatment considered necessary. or After the Service users death if he/she died while still receiving treatment
Inspection reports for boilers, Lifts, etc	Lifetime	Normally lifetime of the installation, but necessary to assess whether there are any Obligations incurred during the lifetime Which may not be invoked until afterwards. If there is a risk then retain inspection reports
Invoices	6 Years	
Job Advertisements	1 Year	
Job applications (following Termination of employment)	3 Years	
Job descriptions (following Termination of employment)	3 Years	
Leavers dossiers (summary)	6 Years	
Ledgers	6 Years	
Litigation Dossiers (complaints/ Accidents)	10 Years	Or as advised by legal representative

<b>TYPE OF RECORD</b>	<b>RETENTION PERIOD</b>	<b>NOTES</b>
Meeting Minutes (Board)	Permanent	
Mortgage documents (acquisition, Transfer and disposal)	Permanent	
Pay Roll	6 Years	
PAYE Records	6 Years	
Property Acquisitions	Permanent	
Property Disposal	Permanent	
Quality Assurance records	12 Years	
Receipt for registered and Recorded delivery mail	1.5 Years	
Receipts	6 Years	
Record of custody & transfer of keys	1.5	
Software Licences	Lifetime	
Study leave applications	1.5	
Tax Forms	6 Years	
VAT records	6 Years	
Wages/salary records	6 years	For Pension purposes it may be Beneficial to keep records until the Person reaches retirement age

**February 2003**

**Reviewed September 2004**

**Reviewed August 2008**

**Next review due August 2011**

### **PRINCIPLES OF THE DATA PROTECTION ACT 1998**

This act gives individuals more rights to see the information held about them and rights of access to the manual files held. Individuals have a right to have any information about them corrected or erased if it is found to be incorrect. They also have a right to prevent information being processed if it is likely to lead to personal damage or distress.

Organisations must ensure that personal data is protected against unlawful or accidental loss, change, disclosure or access. There is also a duty to inform individuals for what purpose Personal data is used and who it is disclosed to.

Principles of the Act:

1. Personal Information shall be obtained and processed fairly and lawfully
2. Personal data shall only be obtained for one or more specified and lawful purpose, and shall not be processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they wee processed.
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data shall not be held for longer than necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act. An individual shall be entitled to:
  - Be informed if personal data is held about them
  - Have access to that data and, where appropriate to have such data corrected or erased
7. Appropriate security measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal date
8. Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data

### **Exemptions from Disclosure**

Under the Data Protection (Subject Access Modification) (Health) Order 2000, paragraph 5 access must not be given to any part of a health record which, in the opinion of the record:-

- Would be likely to cause serious harm to the physical or mental health or condition of the Service user or of any other individual
- Relates to or has been provided by a third party who could be identified from that information, unless that individual consents to the application, or it is reasonable to give access to the information without that consent;

- Where access to any part of a record, in the opinion of the holder, would disclose information provided by a Service user in the expectation that it would not be disclosed to the applicant or information obtained as a result of any examination or investigation to which the Service user consented in the expectation that the information would not be disclosed.

Discretion can be used by the holder of the record regarding disclosure of records where it is:

- Required by statute or court order
- Passing information can be justified in the best interest of the individual or the public. Examples include assisting the police during the investigation of a serious crime, Public Health (control of Disease) Act 1984, Prevention of Terrorism Act 1989, Regulations under the Health and Safety at Work Act 1974.

**RECORDS TO BE KEPT IN HOMES CONCERNING EACH RESIDENT**

1	SERVICE USERS ASSESSMENT
2	SERVICE USERS PLAN (Including Personal Profile ;Risk Assessments; 24hour/weekly plans; Health Safety & Well-being Plan
3	SERVICE USERS PHOTOGRAPH
4	THE NAME, ADDRESS, DATE OF BIRTH AND MARITAL STATUS AND WHETHER THE SERVICE USER IS THE SUBJECT OF ANY COURT ORDER
5	THE NAME, ADDRESS AND TELEPHONE NUMBER OF THE SERVICE USER'S GP AND OF ANY OFFICER OF THE LOCAL SOCIAL SERVICES AUTHORITY WHOSE DUTY IT IS TO SUPERVISE THE WELFARE OF THE SERVICE USER
6	THE DATE OF ADMISSION
7	THE DATE OF DISCHARGE
8	IF THE SERVICE USER IS TRANSFERRED TO ANOTHER HOME OR TO HOSPITAL, THE NAME OF THE HOME OR HOSPITAL AND THE DATE ON WHICH THE HE/SHE IS TRANSFERRED
9	THE DATE, TIME AND CAUSE OF DEATH OF A SERVICE USER
10	THE NAME AND ADDRESS OF ANY AUTHORITY, ORGANISATION OR OTHER BODY WHICH ARRANGED THE SERVICE USERS ADMISSION TO THE HOME
11	A RECORD OF ALL MEDICINES KEPT IN THE HOME FOR THE SERVICE USER AND THE DATE ON WHICH THEY WERE ADMINISTERED TO HIM/HER
12	A RECORD AF ANY ACCIDENT AFFECTING THE SERVICE USER IN THE HOME AND OF ANY OTHER INCIDENT IN THE HOME WHICH IS DETRIMENTAL TO THE HEALTH OR WELFARE OF THE HIM/HER, WHICH RECORD SHALL INCLUDE THE NATURE, DATE AND TIME OF THE ACCIDENT OR INCIDENT, WHETHER MEDICAL TREATMENT WAS REQUIRED AND THE NAME OF THE PERSONS WHO WERE RESPECTIVELY IN CHARGE OF THE HOME AND SUPERVISING THE SERVICE USER
13	A RECORD OF ANY SPECIFIC HEALTH INTERVENTION PROVIDED TO THE SERVICE USER INCLUDING A RECORD OF HIS/HER CONDITION AND ANY TREATMENT OR SURGICAL INTERVENTION
14	DETAILS OF ANY SPECIALIST COMMUNICATION NEEDS OF THE SERVICE USER AND METHODS OF COMMUNICATION THAT MAY BE APPROPRIATE TO HIM/HER
15	DETAILS OF ANY PLAN RELATING TO THE SERVICE USER IN RESPECT OF MEDICATION, NURSING, SPECIALIST HEALTH CARE OR NUTRITION
16	A RECORD OF INCIDENCE OF PRESSURE SORES AND OF TREATMENT PROVIDED TO THE SERVICE USER
17	A RECORD OF FALLS AND OF TREATMENT PROVIDED TO THE SERVICE USER
18	A RECORD OF ANY PHYSICAL INTERVENTION USED WITH THE SERVICE USER
19	A RECORD OF ANY LIMITATIONS AGREED WITH THE SERVICE USER AS TO HIS/HER FREEDOM OF CHOICE, LIBERTY OF MOVEMENT AND POWER TO MAKE DECISIONS

## OTHER RECORDS TO BE KEPT IN ALL HOMES OR AT HEAD OFFICE AS SHOWN

	TYPE OF RECORD	IN THE HOME	HEAD OFFICE
1	A COPY OF THE STATEMENT OF PURPOSE	✓	
2	A COPY OF THE SERVICE USERS GUIDE	✓	
3	A RECORD OF ACCOUNTS KEPT IN THE HOME	✓	✓
4	A COPY OF ALL INSPECTION REPORTS	✓	
5	A COPY OF ANY REPORT MADE UNDER REGULATION 26(4)(c)	✓	
6	<p>A RECORD OF ALL STAFF EMPLOYED IN THE HOME INCLUDING IN RESPECT OF EACH PERSON EMPLOYED:</p> <p><b>FULL NAME, ADDRESS, DATE OF BIRTH, QUALIFICATIONS AND EXPERIENCE</b></p> <p><b>A COPY OF THE BIRTH CERTIFICATE AND PASSPORT</b></p> <p><b>A COPY OF EACH REFERENCE OBTAINED IN RESPECT OF HIM/HER</b></p> <p><b>THE DATE ON WHICH HE/SHE COMMENCES &amp; CEASES TO BE EMPLOYED</b></p> <p><b>THE POSITION HE HOLDS, THE WORK THAT HE/SHE PERFORMS &amp; THE NUMBER OF HOURS HE/SHE IS EMPLOYED EACH WEEK</b></p> <p><b>CORRESPONDENCE, REPORTS, RECORDS OF DISCIPLINARY ACTION AND ANY OTHER RECORDS IN RELATION TO HIS/HER EMPLOYMENT</b></p>		✓
7	A COPY OF THE DUTY ROSTER OF PERSONS WORKING IN THE HOME AND A RECORD OF WHETHER THE ROSTER WAS ACTUALLY WORKED	✓	
8	A RECORD OF THE HOMES CHARGES TO SERVICE USERS, INCLUDING ANY EXTRA AMOUNTS PAYABLE FOR ADDITIONAL SERVICES NOT COVERED BY THOSE CHARGES, AND THE AMOUNTS PAID BY OR IN RESPECT OF EACH SERVICE USER		✓
9	<p>A RECORD OF ALL MONEY OR OTHER VALUABLES DEPOSITED BY A SERVICE USER FOR SAFEKEEPING OR RECEIVED ON THE SERVICE USERS BEHALF, WHICH</p> <ul style="list-style-type: none"> <li>• SHALL STATE THE DATE ON WHICH THE MONEY OR VALUABLES WERE DEPOSITED OR RECEIVED, THE DATE ON WHICH ANY MONEY OR VALUABLES WERE RETURNED OR USED AT THE REQUEST OF THE SERVICE USER, ON HIS/HER BEHALF AND, WHERE APPLICABLE, THE PURPOSE FOR WHICH THE MONEY OR VALUABLES WERE USED <b>AND</b></li> <li>• SHALL INCLUDE THE WRITTEN ACKNOWLEDGEMENT OF THE RETURN OF THE MONEY OR VALUABLES.</li> </ul>	✓	✓
10	A RECORD OF ALL COMPLAINTS MADE BY THE SERVICE USER OR REPRESENTATIVES OR RELATIVES OF SERVICE USERS OR BY PERSONS WORKING AT THE HOME ABOUT THE OPERATION OF THE HOME, AND THE ACTION TAKEN BY THE HOME MANAGER IN RESPECT OF SUCH A COMPLAINT	✓	
11	<p>A RECORD OF ANY OF THE FOLLOWING THAT OCCUR IN THE HOME:</p> <ul style="list-style-type: none"> <li>• ANY ACCIDENT</li> <li>• ANY INCIDENT WHICH IS DETRIMENTAL TO THE HEALTH OR WELFARE OF A SERVICE USER INCLUDING THE OUTBREAK OF INFECTIOUS DISEASE IN THE HOME</li> <li>• ANY INJURY OR ILLNESS</li> <li>• ANY FIRE</li> <li>• ANY THEFT OR BURGLARY</li> </ul>	✓	✓

	<b>TYPE OF RECORD</b>	<b>IN THE HOME</b>	<b>AT HEAD OFFICE</b>
12	RECORDS OF THE FOOD PROVIDED FOR SERVICE USERS IN SUFFICIENT DETAIL TO ENABLE ANY PERSON INSPECTING THE RECORD TO DETERMINE WHETHER THE DIET IS SATISFACTORY, IN RELATION TO NUTRITION AND OTHERWISE, AND OF ANY SPECIAL DIETS PREPARED FOR INDIVIDUAL SERVICE USERS	✓	
13	A RECORD OF EVERY FIRE PRACTICE, DRILL OR TEST OF FIRE EQUIPMENT(INCLUDING FIRE ALARMS) CONDUCTED IN THE HOME AND OF ANY ACTION TAKEN TO REMEDY DEFECTS IN THE FIRE EQUIPMENT.	✓	
14	A STATEMENT OF THE PROCEDURE TO BE FOLLOWED IN THE EVENT OF A FIRE	✓	
15	A STATEMENT OF THE PROCEDURE TO BE FOLLOWED IN THE EVENT OF ACCIDENTS OR IN THE EVENT OF A SERVICE USER BECOMING MISSING	✓	
16	A RECORD OF ALL VISITORS TO THE HOME INCLUDING THE NAMES OF VISITORS	✓	

