

Care In Hand Ltd

General Data Protection Regulation (GDPR)

Confidentiality, Record Keeping and Data Protection

This policy cover the following items:

1. Access to Employee Data
2. Applications for Access to a Deceased Service User's Care Records
3. Caldicott Principles
4. CCTV in Service Users' Homes
5. Confidentiality of Service Users' Information
6. Document Tracking
7. Protecting Personal Data under the General Data Protection Regulation
8. Record Keeping
9. Sharing Information with Other Providers
10. Records Kept in Service Users' Homes

ACCESS TO EMPLOYEE DATA

Care In Hand aims to fulfil its obligations under the Data Protection Act 1998 to the fullest extent.

OUR PROCEDURE

1. Employees are allowed to have access to personal data about them held under the Data Protection Act 1998. This Act requires Care in Hand to respond to requests for access to personal data within 40 days.
2. Details of an employee's personal data are available upon request in accordance with the principles of the Data Protection Act 1998 (see paragraph 1, above).
3. Employees are required to read this information carefully and inform Care in Hand's HR Coordinator at the earliest opportunity if they believe that any of their personal data are inaccurate or untrue, or if they are dissatisfied with the information in any way.
4. The Data Protection Act 1998 gives data subjects the right to have access to their personal data on request at reasonable intervals. Care in Hand believes that complying with a request for a copy of the data annually will satisfy this requirement. Should employees wish to request access to their personal data, the request must be addressed to Mr. Delan Umanee or via email at delan@careinhand.co.uk . The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.
5. In the event of a disagreement between an employee and Care in Hand regarding personal data, the matter should be taken up under the Care in Hand's formal grievance procedure.

ADDITIONAL CLAUSE(S)

1. Where employees make additional requests for access to their personal data which are granted, a fee of £10.00 will be charged which must be paid to Care in Hand before a copy of the personal data will be given.
2. In the interests of openness and fairness, Care in Hand will provide copies of personal records held manually to employees during the month of February each year. The procedure which applies to computerized data will apply to such manual files.

APPLICATIONS FOR ACCESS TO A DECEASED SERVICE USER'S CARE RECORDS

GUIDANCE

It should be noted that the Data Protection Act 1998 does not cover the records of deceased people, and what guidance there is concerns applications to see medical records rather than care records. However, it is reasonable to think that the same principles governing applications to have access to medical records apply equally to care records (and in fact they might overlap).

These principles are that:

1. the medical/care records of a deceased person should be treated with the same degree of confidentiality as for a person who is alive, and
2. where someone applies for access, they must have a good reason and their request is dealt with on a "need to know basis" as if the person were alive.

In respect of medical records, any person with a claim arising from the death of a patient has a right of access to information covered by the Data Protection Act 1998, providing it is directly relevant to that claim. No information which is not directly relevant to the claim may be released.

Thus, a personal representative or executor can access information to benefit the deceased's estate, as can an individual who was a dependent of the deceased and who has a claim relating to that dependency which has arisen from the death.

There are certain exemptions to this right, and information may be withheld if, for example, it identifies a third party without that person's consent or the person gave the information in the past on the understanding that it would be kept confidential.

AIM OF THE POLICY

From time to time Care in Hand might receive an application from a third party, e.g. a relative or solicitor, to have access to the care records of a service user who has died in the course of receiving a domiciliary care service. Current care regulations require all records kept on a service user to be retained for not less than three years from the date of the last entry.

This policy therefore applies primarily to records that have been retained by Care in Hand within this statutory period. The policy determines the actions to be taken in the event of someone requesting access to the deceased person's records during the time that Care in Hand is required to retain them.

POLICY STATEMENT

1. Care in Hand accepts that under certain circumstances a third party will apply for and have the right to have access to the care records of a deceased service user.
2. We will carefully consider any such application but, if unsure about the reasonableness and legitimacy of the request, reserves the rights to take further advice, eg from the Care Inspectorate Wales, or legal advice and to refuse the request altogether. This decision does not prevent the applicant from seeking a court order to disclose the care records.

3. Once we are satisfied that the applicant is entitled to the information, it will provide it within a specified time limit of 21 days.
4. We will give access by allowing the applicant to inspect the records or to extract or to supply a copy if this is requested. In doing so, it recognizes that it will, in line with data protection requirements, need to protect (e.g. by redactions, removal or obtaining consent) information regarding anyone living that is included or referred to in the records.
5. In considering any request, we will consider any information we have on the deceased person's wishes and will act upon these.
6. We might seek to recover the costs of supplying the information, e.g. for photocopying, printing and postage.

CALDICOTT PRINCIPLES

This policy relates to the sharing or transfer of data within NHS or social care organisations, including hospitals, local authorities and GP services. It should be read in conjunction with our separate policies and procedures on GDPR, confidentiality and data management.

THE DATA PROTECTION ACT

Care in Hand recognises that it has a legal duty under the Data Protection Act 1998 to ensure the security and proper management of personal data and that this duty applies to its management, processing and storing of records and data, including information, data and notes about service users. Central to the Act is compliance with data protection principles which are designed to protect the rights of individuals about whom personal data is processed, whether this is via electronic or paper records.

The eight Data Protection principles state that we should make sure that personal information about people is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection.

Care in Hand data protection policies and procedures are designed to comply fully with the Act and these principles. However, we also recognise that a further set of additional data protection principles apply to the NHS and social care, the Caldicott Principles.

THE CALDICOTT REPORT

In 1997, the original Caldicott Report provided guidance to the NHS on the use and protection of personal confidential data and, due to the sensitive and personal nature of medical information in particular, emphasised the need for additional controls over the availability of such information and access to it. The report recognised the importance in a medical and care context of sharing relevant health-related information and made a series of recommendations to ensure that such sharing took place in a way that protected the rights of patients. This led to the requirement for all NHS organisations to appoint a Caldicott Guardian who is responsible for compliance with the principles.

In 2002, the government decided that these standards should be extended to “councils with social service responsibilities” in order to provide a foundation for joint working between health and social services. HSC 2002/003: LAC(2002)2 Implementing the Caldicott Standard Into Social Care was subsequently published.

A further review of the Caldicott Principles took place during 2012 and *The Information Governance Review – To share or not to share* was published.

The revised Caldicott Principles are as follows.

- Principle 1 — justify the purpose(s) for using confidential information.
- Principle 2 — only use confidential information when absolutely necessary.
- Principle 3 — use the minimum information that is required.
- Principle 4 — access to confidential information should be on a strict need-to-know basis.
- Principle 5 — everyone must understand their responsibilities.
- Principle 6 — understand and comply with the law.
- Principle 7 — the duty to share personal information can be as important as the duty to have regard for patient confidentiality.

Care in Hand understands that health and social care professionals should have the confidence to share information in the best interests of their patients and service users within the framework set out by these principles.

PERSON IDENTIFIABLE INFORMATION

With reference to both the Data Protection Act and the Caldicott guidelines, this we recognise person-identifiable confidential information as including:

- a service user’s name, address, full postcode and date of birth
- a service user’s NHS number and any notes, records or information about their care or treatment
- any pictures, photographs, videos, audio recordings or other images of service users
- anything that may be used to identify a service user directly or indirectly, such as rare diseases, drug treatments or statistical analyses using small sample sizes that may allow individuals to be identified.

Importantly, we recognises that person identifiable information does not only relate to medical information and can take many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

We understand that overall there should be a balance between the protection of patient information and the use and sharing of this information between agencies to improve care.

POLICY

Care in Hand recognises that:

- We are required to have a data controller or manager who has overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the Data Protection Act 1998. The Data Controller for Care in Hand is Mr. Delan Umanee

- NHS organisations and local authorities will have an allocated Caldicott Guardian who is responsible for agreeing and reviewing protocols for governing the transfer and disclosure of personal confidential data about patients and service users.
- A Caldicott Guardian is a senior health or social care person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
- The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.
- NHS and Social Care Caldicott Guardians are required to be registered and there is a UK Council of Caldicott Guardians made up of guardians from health and social care.

Within Care in Hand:

- Managers and staff will comply fully not only with the eight principles of the Data Protection Act 1998, but also with the seven Caldicott Principles and with the common law duty of confidentiality. This means that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual concerned. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.
- Service users will be told exactly what their personal information will be used for and how it will be stored and shared. This means fully describing how the data will be used and taking into consideration any language requirements or barriers to understanding, such as requirements under the Mental Capacity Act 2005.
- Care in Hand and its staff have a legal and ethical duty to safeguard the integrity, confidentiality, and availability of sensitive person identifiable information. Every use of person identifiable information must be lawful. Individual service users have a right to believe and expect that private and personal information given in confidence will be kept securely and used only for the purposes for which it was originally given and consented to.
- Staff and managers must be aware of the Caldicott Principles that will apply to any data exchange – they should be aware that NHS organisations and local authorities will have a Caldicott Guardian who will be required to agree to the exchange of person identifiable information.
- Staff and managers must ensure that, to comply with the Caldicott guidelines:
 - Every proposed use or transfer of person identifiable information within or from this organisation should be clearly defined and justified.
 - Personal identifiable information should not be used unless it is absolutely necessary and there is no alternative.
 - Where use of person identifiable information is considered to be essential, the minimum necessary personal identifiable information should be used and each individual item of personal information should be justified with the aim of reducing identity.
 - Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
 - Access to personal identifiable information should be on a strict “need to know” basis. Only those individuals who need access to person identifiable information

should have access to it and they should only have access to the personal information items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes.

- Managers should ensure that everyone is aware of their responsibilities and that a culture of care and due diligence for data security is in place. Actions should be taken to ensure that all staff who handle person identifiable information are aware of their responsibilities and obligations to respect confidentiality.
- Managers and staff should attend data protection and information governance training as required and to a level relative to the requirements of their role. All new staff should read this policy and Care In Hands GDPR policy and comply fully with them and with all related procedures.
- Any data breaches, including breaches of confidentiality, should be reported immediately on being discovered and should be fully investigated. A report should be submitted to Mr Delan Umanee.
- Data sharing arrangements should be regularly audited, with support and guidance obtained from the relevant local authority Caldicott Guardian wherever necessary.

CCTV IN SERVICE USERS' HOMES

POLICY STATEMENT

This policy is written to explain the response of Care in Hand's to the use of closed-circuit television (CCTV) and similar devices such as webcams inside and/or outside the homes of its service users, which record the actions of its staff while working, including when entering and leaving the home.

It should be used with reference to the agency's policies on Data Protection and Stress at Work.

Care in Hand understands that visual images such as photographs and video recordings are defined as data and are covered in the same way as written records by data protection principles in organisations, where the Data Protection Act 1998 applies. However it also understands that private dwellings are not covered by the Data Protection Act, which means that the guidance produced by the Information Commissioner's Office on the use of CCTV does not extend to its use in private households.

Care in Hand recognises that it is providing a social service, which in line with its registration responsibilities, has a duty to make sure on the one hand that its service users are kept safe from harm and on the other that its staff are not subject to undue harassment or pressures that could impair the quality of their care and their welfare.

We are therefore aware that service users, relatives and representatives might seek to use CCTV and similar devices to record the care being given to service users as a protective measure, but this might also have the effect of increasing staff stress and be counterproductive in terms of achieving the standards of care that are expected of them.

We have therefore devised our own Code of Practice, which it applies in those homes where it knows that CCTV or similar devices have been installed (or are planned to be installed), which could record the actions of its staff while carrying out their caring duties. The code does not apply to houses where CCTV has been installed for external security purposes only and which would not record such as times of workers entering or leaving the house. It does apply where such actions are routinely recorded.

CODE OF PRACTICE

The code is written to reflect the responsibilities of users of surveillance methods in their relationships with other parties who might wittingly or unwittingly be exposed to them as described in the Information Commission Office guidance on the use of CCTV in organisations where data protection principles apply.

Care in Hand follows the following principles.

1. We acknowledge that any CCTV and similar recording devices belong to the service user/representatives and it has no control over their use. It can, however, negotiate how they are used in relation to the services, which we have agreed to provide. We enter into any negotiations with a view to creating relationships with the service user and their representatives, which are based on mutual trust, openness and transparency.
2. We also recognize that video recording can be a useful tool to help protect a service user from harm and the risk of harm, to promote learning and development and to improve the quality of care if used appropriately.
3. We work on the basis that care practices must only be recorded on CCTV and similar devices with the express permission of the Director of Care in Hand and individual carers.
4. Service users/representatives who seek to make use of CCTV within the service delivery process must make this clear at the beginning of the service or when proposing it at any later stage so that its use and conditions of its use can be written into the service agreement.
5. Representatives of a service user who seeks to install or use CCTV on behalf of the actual service user must have obtained the latter's permission or if the person lacks mental capacity to give their consent, the agency will insist that a "best interests" process is carried out.
6. Where any such agreement has been reached, Care in hand will then make the relevant staff aware of its use and obtain their written consent to their being recorded.
7. We will always seek to establish the purpose of the use of the CCTV (which might not always be directed at our staff, but a means, for example, of checking on the service user her or himself). It will then set out in writing the purpose and any specific objectives, which are relevant to the individual care and support plan.
8. Care in Hand will not agree to the routine recording of any intimate personal care that invades the privacy of the service user and affronts their dignity.
9. Care in Hand's Directors could agree to certain aspects of the care provided to be recorded (with consent) for a specific purpose, e.g. for problem-solving or learning, where there are benefits of recording the procedure for both service user and staff.
10. Care in Hand will not seek to make use of the recording for its own internal monitoring purposes.
11. We will discuss with the service user/representatives as part of the agreement on the use of the CCTV how long the images of its staff will be retained, what access other people might have to those images and how they will be disposed of. These are all matters that could affect the rights of Care in hand's employees.
12. We will also come to some agreement with the service user/representatives as part of the agreement the rights of access of its staff to any recorded images of them, as they would if the process was following data protection principles.
13. Care in Hand will not tolerate the use of covert surveillance of its staff by a service user and/or their representatives, which implies lack of trust and confidence in both individual staff and the agency. If it discovers that covert surveillance methods are being used unilaterally and without adequate reasons it will discuss ending its services to that user.

14. Under some circumstances, however, it would accept the results of covert recordings if they provide clear evidence of malpractice or misconduct on the part of the staff member being recorded or to support a complaint.
15. In exceptional circumstances where, for example, there is prior evidence of an agency employee harming the service user in any way or putting the person at risk of harm or engaging in any other kind of possible misconduct it might agree with the service user/representatives to staff behaviour being recorded covertly. The evidence obtained could then be used to trigger the agency's safeguarding procedures.
16. The agency accepts that each situation should be treated differently and the agreements reached will be on an individual basis.

CONFIDENTIALITY OF SERVICE USERS' INFORMATION

POLICY STATEMENT

Care in Hand works on the principle that it has a duty of confidentiality to its service users. The service regards this as being of the utmost importance and a key part in building a trusting, caring environment where service users are safe in the knowledge that their confidences will be kept and where information about them will be protected safely. Our policy states that all the information we receive about or from service users is confidential and that only those people who need to know the information will have access to it. We will always seek the written permission of its users prior to sharing personal information about them with anyone else.

Care in Hand complies with Care Inspectorate Wales guidance, which requires the registered manager of a service to make sure that service users know that information about them is handled appropriately, and that their confidences are kept.

PROCEDURES

To comply with this policy Care in Hand's staff must:

1. 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 who have a need and a right to access them (see also the policy on Record Keeping)
2. wherever practical or reasonable fill in all care records and service users' notes in the presence of and with the co-operation of the service user concerned
3. ensure that all care records and service users' notes, including care plans, are signed and dated.

Rare situations may arise which give rise to exceptions to this duty where confidential information may relate to harm to other service users or harm to the person sharing the confidence. In such circumstances we reserve the right for staff to break their duty of confidentiality and to take the information to a senior member of staff. In such rare circumstances:

1. the relevant service user will be informed of the service's position and full details will be discussed with the service user
2. appropriate notes will be made in the service user plan and these notes will be open to inspection by the service user
3. the information will only be given to those who absolutely need to know and wider issues of confidentiality of that information will still apply
4. the service user will be free to make a complaint through the service's complaints procedure if he or she considers that the information held about them has not been treated in the confidential manner they should expect.

DOCUMENT TRACKING

Staff Documentation & Transporting Service User information

Re: Taking Hard Copy data away from Care in Hand Premises.

- 1) While performing duties it is anticipated that data will be taken away from Care in Hand offices, we need to ensure the below policies are considered and adhered to in order to comply with GDPR regulations.
- 2) This material should only be taken from Care in Hand offices when it is a necessity
- 3) This information must be kept confidential at all times.
- 4) Where data contained within paper records is needed to be taken from a Care in Hand office, this should be kept to a minimum both in terms of content and duration. Consider how much information is required for that particular service user or to complete the relevant task and avoid taking unnecessary information.
- 5) Where paper records are in transit from a Care in Hand office to another location i.e a service users address, they should be transported in a way that mitigates against the risk of confidential information being obtained by unauthorised parties.
- 6) Where data is taken from a Care In Hand office, ensure it is tracked in accordance with our document tracking log at all times.
- 7) If you become aware of any breach or potential breach you must inform Delan Umanee immediately
- 8) If you have any further queries then do not hesitate to get in touch with Delan Umanee Data Controller

Client Documentation

Due to the nature of the organisation, Care in Hand staff are regularly required to transport documents such as care plans and communication books between locations which may include your personal data. We would therefore like to reassure you that Care In Hand take data security very seriously and have a number of procedures in place to secure your data when it is being transported outside of Care in Hand offices. In particular we have a document tracking log whereby staff are required to ensure that whenever data is taken from a Care in Hand office or your premises for any reason, it is logged in the document tracking log at all times so that the handler of those documents is known at all times. If you are at any point concerned about the security of your data, please do not hesitate to contact Delan Umanee immediately on delan@careinhand.co.uk or 01834811333

Mimecast

Secure messaging technology is essential to safeguarding sensitive information shared with colleagues and partners via email. For data such as financial records and customer information, secure messaging helps to prevent inadvertent or deliberate data leaks and protect valuable information in transit.

Care in Hand's Process:

When users want to send a protected message, they simply create a new email and then choose the Send Secure option within the Mimecast for Outlook secure email tab. Before clicking send, they select administrator-defined options that include requiring a read receipt, setting message expiration dates, and restricting printing and replying.

Once the message is sent, the email and attachments are uploaded to the Mimecast cloud, scanned for viruses and checked against data leak prevention policies before being stored in a secure AES encrypted archive.

The message recipient then receives a notice with instructions for logging into the Mimecast secure web portal where they can retrieve the message, download attachments and reply to the message securely as well.

Additionally, Secure Messaging are initiated when the content of an email meets certain policies applied at the email security gateway.

INITIAL ASSESSMENT POLICY

New service users and prospective service users are shown a copy of the statement below and have it explained to them and their representatives so that they can understand it as fully as possible and sign it.

Every effort is made by staff to ensure that service users fully understand the implications of the policy. The member of staff performing the assessment is expected to ensure that the new service user understands and has read the following statement.

“To help us make an assessment of your needs, we will need to ask you for personal information about your circumstances and to record this information. We will not share this information with anyone, including friends and relatives, without your agreement (unless they have legal authority as Guardian or Attorney) and it will be kept in a confidential file which will be kept in a locked filing cabinet.

Only care staff with permission to see the file will be able to access it. Care staff will record in the file on a daily basis information relevant to your care and will pass on information relevant to your day-to-day care to your key worker or to whoever is in charge of each shift.

You may have access to your notes at any time to see what is actually being recorded. It is Care In Hand’s that all the information we receive about or from service users is confidential and that only those people who need to know the information will have access to it.

We will always ask your permission before we share with anyone else the information you have given us. In certain circumstances, however, we may need to share information in your best interests and may do so to fulfil our duty of care to you to keep you safe from risk of harm by following the procedures that are set out in the service’s safeguarding policy.”

Signed (service user/lawful representative):

Countersigned (manager/representative): Date:

REQUESTS FOR INFORMATION

Care in hand will not provide information to relatives, spouses, friends or advocates without the consent of the individual service user concerned. If the person is unable to give their consent a decision will be taken in line with “best interests” procedures set by the Mental Capacity Act 2005.

All enquiries for information, even if they are from close relatives, should be referred back to the service user or the service user’s permission sought before disclosure. If the relative or person who seeks to have access to this information objects to the decision they will be asked to make a formal written complaint, which will be addressed through the service’s complaints procedure.

The service is also often asked for reports by insurance companies, solicitors, employers, etc. Before providing these reports we shall require written consent from the service user concerned and will never divulge information without consent unless obliged to by law.

RECORD KEEPING

We keep files on all our service users but only keep relevant information to ensure that the care we offer as an organisation is of the highest quality. The files are only available to staff who need to use them. We keep very personal letters or notes in a secure place.

Care in Hand makes sure that:

1. records required for the protection of service users and for the effective and efficient running of the service are maintained, are up to date and are accurate
2. service users have access to their records and information about them held by the service, as well as opportunities to help maintain their personal records
3. individual records and care service records are kept in a secure fashion, are up to date and in good order; and are constructed, maintained and used in accordance with the Data Protection Act 1998 and other statutory requirements.

We consider that access to information and security and privacy of data is an absolute right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

Under the Data Protection Act 1998 the service should have a nominated data user/data controller.

The data user/data controller for this service is Mr. Delan Umanee

PROTECTING PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION

AIM AND SCOPE

This policy shows how we comply with the requirements of the data protection requirements found in Regulation 17: Good Governance of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which expects service providers to have effective governance of their record keeping with records that are comprehensively fit for purpose and securely maintained.

The policy applies to all manual and electronic records kept by the service in relation to service users, including those involved with them, whose personal data might be found on their records, all staff, and any third parties (agencies and professionals), with whom anyone's personal data information held by the service might have to be disclosed or shared.

The policy should be used with other relevant record-keeping policies on:

- Applications for Access to a Deceased Service User's Care Records
- Confidentiality of Service Users' Information
- Information Governance under the General Data Protection Regulation, which addresses the wider organisational and management of information issues
- Record Keeping, which addresses the practice of record keeping
- Service Users' Access to Records.

POLICY STATEMENT

Care in Hand recognises it must keep all records required for the protection and wellbeing of service users, and those for the effective and efficient running of the care service such as staff records to comply currently with the Data Protection Act 1998 and its successor Act, when

passed by Parliament, and the EU General Data Protection Regulation (GDPR), which comes into force from May 2018 (and which is likely to apply post-Brexit).

In line with its registration under the Data Protection Act, and to comply with the GDPR, the service understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

This means that all personal data obtained and held by the care service to carry out its activities as a registered care provider must:

- have been obtained fairly and lawfully
- held for specified and lawful purposes as an organisation that is carrying out a public duty
- processed in recognition of persons' data protection rights, which are described in the GDPR in terms of the right:
 - to be informed
 - to have access
 - for the information to be accurate and for any inaccuracies to be corrected
 - to have information deleted (e.g. if inaccurate or inappropriately included)
 - to restrict the processing of the data to keep it fit for its purpose only
 - to have the information sent elsewhere as requested or consented to (e.g. in any transfer situation)
 - to object to the inclusion of any information (e.g. if considered to be irrelevant)
 - to regulate any automated decision-making and profiling of one's personal data.
- be adequate, relevant and not excessive in relation to the purpose for which it is being used
- be kept accurate and up to date, using whatever recording means are used or agreed (eg manual or electronic)
- not be kept for longer than is necessary for its given purpose (e.g. in line with agreed retention protocols for each type of record)
- have appropriate safeguards against unauthorised use, loss or damage with clear procedures for investigating any breaches of the data security
- comply with the relevant GDPR procedures for international transferring of personal data.

PROCEDURES

Care in Hand have therefore taken the following steps to protect everyone's personal data, which it holds or to which it has access so that it complies with current data protection laws and the GDPR.

1. It appoints or employs staff with specific responsibilities for:
 1. the processing and controlling of data – Mr. Delan Umanee
 2. the comprehensive reviewing and auditing of its data protection systems and procedures – Mr. Delan Umanee
 3. overseeing the effectiveness and integrity of all the data that must be protected
All Care Management/ operational coordinators and management staff

There are clear lines of responsibility and accountability for these different roles. In addition please see our in depth "**Protecting Information under GDPR Policy**"

RECORD KEEPING

POLICY STATEMENT

Every care service is required to have systems and methods for keeping records that comply with its registration conditions as set out and specifically Regulation 16: Records of Personal Plans, Regulation 55: Records and Regulation 74: Duty to ensure there are systems in place for Keeping of Records and the General Data Protection Regulation (GDPR), which applies to all business and organisations that process personal data.

This policy is intended to set out the values, principles and policies underpinning Care in Hands approach to record keeping, data protection and access to records.

The policy should be read and used in relation to policies on:

- Applications for Access to a Deceased Service User's Care Records
- Confidentiality of Service Users' Information
- Protecting Personal Data under the General Data Protection Regulation
- Service Users' Access to Records
- Records Kept in Service Users' Homes

Care in Hand works to the following principles of good record keeping.

1. Records required for the protection of service users and for the effective and efficient running of the care service are maintained, are up to date and are accurate.
2. Service users have access to their records and information about them held by the care service, as well as opportunities to help maintain their personal records.
3. Individuals' records and other records that contain private, confidential personal data are kept in a secure fashion, are up to date and in good order, and are constructed, maintained and used in line with the applicable regulations and related policies (see above).

DATA PROTECTION

See the **Protecting Personal Data under the General Data Protection Regulation**.

ACCESS TO RECORDS

Care in Hand considers that access to information and security and privacy of data is an absolute right of every service user and that service users are entitled to see a copy of all personal information held about them and to correct any error or omission in it.

Please see separate Policy on **Access to Service Users Records Policy**

RECORD-KEEPING PROCEDURES

All Care in Hand staff must do the following.

1. Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them. (Where a service user keeps their own records at home the manner of safe storage is discussed with the person concerned and / or where appropriate, their relatives. Confidentiality aspects are discussed as part of the initial assessment process.
2. Be aware that the relatives of a service user do not have any automatic right of access to that service user's files and need to have the service user's permission to see any information on that person. If the service user lacks the mental capacity to give their permission a "best interests" procedure would then need to be followed in line with the Mental Capacity Act 2005.
3. Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
4. Wherever practical or reasonable fill in all care records and service users' notes in the presence of and with the co-operation of the person concerned.
5. Ensure that all care records and service users' notes, including care plans, are signed and dated.
6. Check regularly on the accuracy of data being entered into computers.
7. Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
8. Use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to service users or staff should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the branch manager. Where personal data is recorded on any such device it should be protected by:

1. ensuring that data is recorded on such devices only where absolutely necessary
2. using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
3. ensuring that laptops or USB drives are not left lying around where they can be stolen.

RETENTION OF RECORDS

All records are kept in line with the requirements of the current legislation and guidance. Service users' personal records that have been kept independently by the service are always kept for a minimum of three years from the date of the last entry after they leave the service or after their death.

SHARING INFORMATION WITH OTHER PROVIDERS

POLICY STATEMENT

Care in Hand accepts that to provide the highest standard of care for our service users it is vital to work in partnership with other professionals and services. A key aspect of partnership working is the sharing of relevant information, which in line with confidentiality and data protection rules, should always be on a "need to know" basis.

This policy is intended to set out the values, principles and procedures underpinning the service's approach to sharing information about service users with other providers.

POLICY ON SHARING INFORMATION WITH OTHER PROVIDERS

Care in Hand recognises that its services form one element in the range of care, treatment and support with which its service users need to be engaged, and that, to provide optimal care, it needs from time to time to share information with other health and social care providers. Subject to our obtaining the express consent of service users, including written consent where important, there is a particular responsibility for such information sharing:

- when a prospective service user is considering having domiciliary care
- when a service user needs a specific health service
- when a service user is admitted to or discharged from hospital
- when a service user transfers to another care setting
- towards the end of life.

Sharing information about a service user will only be undertaken with their express permission, but every effort will be made to persuade service users that sharing information on their needs is vital to their care.

STARTING CARE

Around the time when a prospective service user is considering starting to receive care it is important, as part of the comprehensive needs assessment process, that the service becomes aware of information held by other providers and practitioners relating to the person's health and care needs, in order to ensure that the service has the necessary capacity to respond to those needs.

NEEDING A HEALTH SERVICE

When a service user needs a health service, whether this is from a general practitioner, from a hospital, or from some other health professional, it is vital that the body responsible for the treatment has the fullest possible information. The care service, which will often have been in a good position to observe the service user's needs and symptoms, will co-operate as fully as possible in supplying information to responsible health service personnel.

ADMISSION TO AND DISCHARGE FROM HOSPITAL

Care in Hand recognises admission to hospital as a critical event in the life of a vulnerable service user. We will do everything possible to ensure that health service staff have good information about the service user's needs, taking special care with communication when treatment is urgent. This information should include any advance directives, particularly involving DNAR, issued by the person that have been passed on to the care service.

Similarly, when a hospital patient is discharged, whether or not the person has previously been a user of our service, we will make every effort to ensure that it has all of the necessary information about the person's needs to ensure that the transition between environments is achieved with as little disruption in care as possible.

TRANSFER TO ANOTHER CARE PROVIDER

Care in Hand recognises that some service users will wish to move to a different provider, to a care home, or to a situation where they will be more independent but be regularly helped by a relative or friend. In such instances we will co-operate fully in passing information about the service user and their needs to those who will take over care responsibility.

END-OF-LIFE CARE

Care in Hand recognises that the period towards the end of a service user's life is one which makes particular demands on those undertaking care and which calls for especially close co-operation over information sharing. We will pass on to anyone undertaking the terminal care of one of our service users information about both their condition and needs, and any wishes that have been expressed to us about how their care should be handled, including any advance directives that they have issued.

RECORDS KEPT IN SERVICE USERS' HOMES POLICY

POLICY STATEMENT

This policy is intended to set out the values, principles and policies underpinning Care in Hand's approach to record keeping, data protection and access to records in respect of those records that are kept in service users' homes.

This policy is written to achieve National Minimum Standard 16 for Domiciliary Care Agencies in Wales — Records Kept in the Service User's Home.

Care in Hand believes that all records required for the protection of service users and for the effective and efficient running of Care in Hand should be maintained accurately and should be up to date, that service users should have access to their records and information about them and that all individual records and agency records are kept in a confidential and secure fashion.

PROCEDURES

1. With the service user's consent, care workers should record, in records kept in the homes of service users, the time and date of every visit to the home, the service provided and any significant occurrence.
2. Where appropriate, records should include:
 1. assistance with medication — including time and dosage
 2. financial transactions undertaken on behalf of the service user
 3. details of any changes in the service user's or carer's circumstances, health, physical condition or care needs
 4. any accident, however minor, to the service user and/or care or support worker
 5. any other untoward incidents
 6. any other information that would assist the next health or social care worker to ensure consistency in the provision of care.
3. Care in Hand staff should ensure that all written records are legible, factual, signed and dated by the person making the record, and kept in a safe place in the home, as agreed with the service user and their carer, relatives or representative.

4. Care in Hand will ask any service user or their carer, relative or representative on his or her behalf, who refuses to have records kept in their home to confirm the refusal in writing and a record of this is kept on the user's personal file at Care in Hand.
5. Service users should have access to their records and information about them held by Care in hand; they should also be given opportunities to help maintain their personal records.
6. Other records required for the protection of service users and for the effective and efficient running of Care in Hand are maintained in an up-to-date and accurate fashion by all staff.
7. Individual records and Care in Hand records are always kept in a secure fashion, are up to date and in good order; and should be constructed, maintained and used in line with the Data Protection Act 1998 and other statutory requirements.
8. Care in hand policy is to keep the ongoing records in the service user's home for an agreed period (usually one month or until the service is concluded) depending on the frequency of the visits, nature and intensity of the care provided. After the agreed time they are transferred with the permission of the service user, to the office for safe keeping and agency monitoring and reviewing purposes.

Care in Hands staff should:

- wherever practical or reasonable, fill in all care records and service user notes in the presence of and with the co-operation of the service user concerned
- ensure that all care records and notes, including service users' plans, are signed and dated
- Understand the difference between the White, Red and Blue folder systems, shown to them during the Induction Process.
- Ensure that all files or written information of a confidential nature are stored in a secure manner wherever possible.
- Inform the office where a file falls below the standards required (such as tattered or broken folder), where a replacement and updated file will be provided.