Care in Hand
Rely on us to care for you

Care In Hand Ltd

General Data Protection Regulation (GDPR) Policy

Aim and Scope of Policy

This policy shows how Care in hands complies with the requirements of data protection requirements 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
- Access to Employee Data
- Caldicott Principles Policy
- CCTV in Service Users Homes Policy
- 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
- Sharing /Information with other Providers Policy
- Social Media Policy
- 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).

In line with its registration under the Data Protection Act, and to comply with the GDPR, we understand that we 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 Care in Hand 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 (eg 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 (eg in any transfer situation)
  - to object to the inclusion of any information (eg 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 (eg 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 has 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 staff with specific responsibilities for:

Responsibility 1 -The processing and controlling of data – Mr Delan Umanee

Responsibility 2 - the comprehensive reviewing and auditing of its data protection systems and procedures – Mr Delan Umanee

Delan carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the service.

Responsibility 3 - overviewing the effectiveness and integrity of all the data that must be protected.

Care in Hand
Rely on us to care for you

Data Protection Officers

Human Resources Department:	Rhianna Walwyn
Worked Based Learning Department:	Wendy Skeels
Payroll Department:	Nicola Edge
Commissioning Department:	Charlotte Evenden

Officers within each department can account for all personal data it holds, where it comes from, and who it is and might be shared with.

Training Department – Liz Miller

It provides its staff with information and training to make them aware of the importance of protecting people's personal data, to teach them how to do this, and to understand how to treat information confidentially.

All Officers and Care Managers:

Narberth Branch:	Marc Davies
Wooden Branch:	Julia Sharp
Pembroke Branch:	Amanda Stocker
Fishguard Branch:	Fiona Briscoe

1) provide information to its service users and others involved in their care on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions service users and staff can take if they think that their data has been compromised in any way (eg through the complaints procedure or grievance procedure in the case of staff).

2) Recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions.

3) Have policies and procedures for enabling service users and/or staff to have access to their personal information, and for the making of subject access requests that are in line with the GDPR. Formal Access to Records are to be put in writing to **Mr. Delan Umanee**

All Officers have appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences (eg fine).

Care in Hand
Rely on us to care for you

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 user's 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.

Training

New staff must read and understand the policies on data protection and confidentiality as part of their induction.

All staff receive training covering basic information about confidentiality, data protection and access to records.

Training in the correct method for entering information in service users' records is given to all care staff.

The nominated data controller/auditors/protection officers for the care service are trained appropriately in their roles under the GDPR.

All staff who need to use the computer system are trained to protect individual's private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches of the service's policies and procedures.