Clifton Home Care Ltd
30 Orchard Road Lytham St Annes FY8 1PF
Phone: 01253 722945

GDPR01 – General Data Protection Regulations

Please read this in conjunction with our Privacy notice (for staff and clients)

Purpose

To comply with the requirements of the General Data Protection Regulations 2018 and Regulation 5 of the Health Service (Control of Patient Information Regulations) 2022.

Scope

This policy covers all aspects of information obtained and held by Clifton Homecare Ltd (CHCL) including (but not limited to):

- Service user and employees' details, medical history & NOK details
- Personal information provided by clients & families in order that we can deliver our care and support duties
- Employee details to enable a contract of employment to be issued.

Caroline Cosh has been appointed as the Senior Information Risk Owner and is responsible for data protection. Currently Caroline is also the Caldicott Guardian although is in talks with another local care company; to share the role; to minimise conflict.

Policy and Procedure

GDPR identifies the rights of individuals: -

- Right to be informed
- Right of access
- Right to rectification (in CHCL case immediately any discrepancy is identified)
- Right to erasure portability
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making & profiling

Right to be informed

We may collect information or data about you in various ways in order to develop a support and care plan to allow the team at CHCL to meet your needs safely. The main circumstances we do so are noted below: -

- The information obtained from either the client, relative, lasting power of attorney appointee or advocate is used in the formulation of the care plan. All appropriate parties will be encouraged to read the care plan to ensure the information is accurate and correctly documented. These details are stored in a file at the client's location. Any updates to the support and care plan will be documented after approval of the details by yourselves. At the end of each visit and at the time of medication administration the care team will complete notes summarising the duties completed and medication administered. In 2022 all care planning documentation will be made digital via Clifton Homecare's OnePlan software provider. All clients or families will have opportunity to access the care records on

file and recorded by the care team once the digital system is in use. Only people with client/ LPA written consent will have access to this information.

- Our website does not collect details of your IP address and which version of the web browser you used to review our website. We use photographs of some of our clients in our marketing video. This is only with written consent which is retained on file. We retain a photograph of clients within their client file for identification purposes. This may include the Herbert protocol used for people with Dementia in case they go out unsupervised and get lost/ don't return.

Rights of access

We have to request your approval for Clifton Homecare to maintain these personal records. You have a right to access your personal data but we can refuse access to data if we feel your request is unreasonable, repetitive or excessive. **Clifton Homecare will provide information within one month from receipt of request.** We are allowed to charge a reasonable fee to cover admin costs. You will be provided with refusal information, the option to complain to the Information Commissioner's Office (ICO) if you feel a refusal is unjust and if there is a charge for the provision of information this cost will be made clear within the month.

When an individual makes a request they can do so in writing, verbally or even through social media. The request can be made to any member of staff at any time. All staff must record what requests are made and must provide this request to the manager on call. The manager will then need to make this request known to the SIRO who has one month of the request to respond. It is therefore important for this information to be passed to the SIRO at the earliest opportunity.

The SIRO needs to confirm identity of the individual making the request. If the request is complex a two-month extension can be taken but the individual needs to be notified with the first month that this will be the case.

Right to rectification

It is essential for not only health and safety but quality of care delivery for us to maintain accurate records. If you believe any specific information we have obtained is, in your or our opinion incorrect, please inform our administration team and request the information is corrected. Our office manager will help ensure this is completed to your satisfaction and in line with regulatory requirements. If you do remain unhappy with the rectification completed, please contact Clifton Homecare's Senior Information Risk Owner (SIRO) Caroline Cosh; caroline@cliftonhcl.co.uk. If we, as a Company, believe the information is accurate and correct, we will not change the information. You have a right to make a complaint and you can seek to enforce your rights through a judicial remedy. Please refer to our separate Complaints policy and procedure for details. This can be found on our website, in client care folders and be sent to you by our administration team (contact details; cliftonhcl@gmail.com or telephone 01253 722945).

Right to restrict processing

We must have a determined and valid lawful basis to process personal data. Clifton Homecare does process data relating to employees and clients. The data processed and reasons for this are outlined below. If the purpose for processing changes, then the affected individuals will be notified accordingly. Special category data is not processed. Clifton Homecare produces care plans using Windows 10 software. Any information gleaned from a client in relation to production and subsequent

implementation of the care package is appropriate, relevant to the care we provide and used to maintain a client's wellbeing and safety. In 2022 care plans will be made digital and our employees will have access to client's personal, health related and care/ support needs via the OnePlan software. Care team employees will only be able to access information relating to clients that they are attending. The administration team will have access to all client information stored at the office. Information is only processed for the length of the contract. Employee data is processed also only for the length of time that they are an employee with Clifton Homecare. When employment ceases information is no longer processed once final wages have been paid.
We have identified an appropriate lawful basis for processing data and have considered how the processing may affect individuals concerned and can justify any impact. We are open and honest and comply with the transparency obligations of the right to be informed.

Client information processed:

- Weight
- Height
- Fall records
- Accident and incident reporting relating to individuals
- Hospital admission records
- Medication administering and documentation
- Daily recorded information
- Pressure ulcer information

The purpose of client data processing is for quality assurance and health and wellbeing monitoring.

Employee information processed:
Name and date of birth
Current and previous addresses relating to the last 8 years
National Insurance number
Email address
Attachment of earnings information
Criminal record history (the employee must consent to this application and understand that this consent can be withdrawn at any time, but, employment will not be supported without this regulatory check being carried out). Caroline Cosh is ultimately responsible for managing this information and keeping the information secure. Administration staff members only access this information if there is a legitimate reason. All employee files are kept locked in secure cupboards.
The purpose of employee data processing is for payroll; wage calculation, DBS completion for regulatory and Safeguarding purposes and training/ competency systems such as the Digital Medication competency system being trialled by Clifton Homecare, on behalf of Health Education England (2022-2023).

Our payroll processing is undertaken by Forbes Watson Accountants and our DBS checking process is managed by 'On Line DBS' and 'DBScheckonline'. Forbes Watson Accountants and On-Line DBS have their own GDPR policies and procedures. Processing agreements are held on file for Forbes Watson accountants, DBS companies and OnePlan software.

Clifton Homecare reviews all of our data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies.

GDPR01 – General Data Protection Regulations

At this time, we do not share any data for planning or research purposes for which the national data opt-out would apply. We review all of the confidential patient information we process on an annual basis to see if this is used for research and planning purposes. If it is, then individuals can decide to stop their information being shared for this purpose. You can find out more information at https://www.nhs.uk/your-nhs-data-matters/.

Right to data portability

You have the right to get your personal data from Clifton Homecare in a way that is accessible and machine-readable. You also have the right to request that Clifton Homecare transfers your data to another organisation. Please note though that we store a copy of your data relating to the time services were provided to you for a period of 8 years after service provision ceases. In order to request data portability contact us directly; cliftonhcl@gmail.com or 01253 722945 and state clearly what you want. We will request that the request for data portability to be provided in written format (writing or email).

Right to object

The GDPR right to object allows clients and staff to object to certain types of data processing and stop Clifton Homecare from continuing to process their personal data. There are only certain situations when a legitimate right to object can be sent to a company.

These are:

- Direct marketing
- The processing of personal data for statistical purposes related to historical or scientific research
- The processing of data for tasks in the public interest
- The exercising of official authority invested in you
- Objections to data processing in yours or a third party's legitimate interest
- Objections to data processing based on their own beliefs and situations

Clifton Homecare have one month to assess, review and provide feedback to an objection, in accordance with the legitimate right to object.

Rights in relation to automated decision making and profiling

We do not use any automated decision making or profiling software.

Obtaining consent

We may use personal information:

- To provide you with information relevant to your care package and details of any medical practitioner requirements specific to your care
- To notify you of any change to our services we provide for you
- To assist with any contractual obligations
- To allow training courses to be undertaken and any additional training required to be identified
- Supervisory reports completed after regular monitoring of employee performance

GDPR01 – General Data Protection Regulations

Personal and special category of data obtained from client, staff and any other source relevant to our domiciliary care activities may include:

- Racial or ethnic origin of a client or employee
- Their religious beliefs if these will impinge on any care packages we implement
- Their physical and/or mental health condition
- Their sexual life but only so far as this will affect the care package and support we provide
- Name and contact details

We use Cloud based software for maintaining electronic storage information – a secure system, password protected with password changed regularly.

Service user and employee files are locked away when the office is closed. No records are left on desks when the office is unmanned and no paper records are stored in company cars.

Messaging to staff uses a secure password protected WhatsApp software which is encrypted and client details are obtained by the care team using OnePlan software. The care team have to input a password in order to view personal and keysafe information on a secure app.

All passwords are changed regularly and all clients are encouraged to change key-safe codes regularly. Clifton Homecare will assist with this process, if required.

Retention periods of records obtained

- We collect employee information such as their address, contact details, next of kin and any details of any physical concerns that may affect their health and/or wellbeing whilst at work
- The personal data we maintain is kept to a minimum subject to CQC and data retention requirements:
- Client records – 8 years after ceasing to be a client
- Staff records – 8 years after ceasing to be an employee

- Unsuccessful staff application forms – 12 months after vacancy closing date
- Timesheets and financial documents – 8 years
- Employers' liability insurance – 40 years
- All paper-based records that have been superseded and contain an identifier are shredded before disposal.

(Please refer to our Retention Record Policy for further information).

Data Breach Procedure

A data breach is when the information we hold, create, or share (e.g. care records) is compromised. This might be in one of 3 ways:

1. Confidentiality – When a person gains access to information they shouldn't have. This might be malicious i.e. a hacker, or it might be a simple mistake i.e. sending an email to the wrong person;
2. Integrity – we need to know that information is accurate and that it was created by the right person. For example, a MAR sheet needs to have been filled out correctly. If there is an error on the sheet –

whether on purpose or not – this is a data breach; or
3. Availability – for data to be useful we need to be able to access it. If it isn't available this is also a breach, e.g. there is a care record which is needed to provide care for someone, this is kept locked in an office, if the keys go missing and no one can access that record then this is a data breach.

It is better to report a breach even if you are not sure that it is one. As with incident reporting, near misses are as important to report as actual incidents. This is how we learn and can hopefully prevent these things happening in the future.

If a breach has occurred, there are four important elements to any breach management plan:

1.Containment and recovery
2.Assessment of ongoing risk
3.Notification of breach
4.Evaluation and response

First though; if you believe a crime has been committed, someone has been injured or an intruder is on sight contact the emergency services via 999.
Complete an Incident report as soon after the incident as you can so that you can recall factual details. This needs to be given to the SIRO; Caroline Cosh.
If you have identified a potential security breach inform on-call or the office who will notify the SIRO at the earliest opportunity.

1. Containment and recovery

Data breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists acrossthe business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers.

Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach cancause. As well as the physical recovery of equipment, this could involve the use of backup media to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police.

2. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of

incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of an employee database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary, further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and howlikely they are to happen.

The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss ofapparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3. Notification of breaches

Informing people and organisations that we have experienced a data security breach can be an important element in our breach management strategy. However, informing people about a breach is not an end in itself. Notification will have a clear purpose, whether this is to enable individuals who may have been affected to takesteps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.
From 26 May 2011 certain organisations (service providers) have a requirement to notify the InformationCommissioner (ICO), and in some cases individuals themselves, of personal data security breaches. We will report all breaches to the ICO in a timely manner and seek support when needed from our IT and software supplier/ support network.

For more information about the specific breach notification requirements for service providers see: ICO

GDPR01 – General Data Protection Regulations

- Answering the following questions will assist other types of organisations in deciding whether to notify:

  - Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances. Health and Social Care providers will have a legal responsibilityto notify their Regulator of breaches, and may have a contractual obligation to notify commissioners of services, such as Social Services or NHS.
  - Can notification help you meet your security obligations with regard to the seventh data protection
    principle? This is "Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."
  - Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act
    on the information you provide to mitigate risks, for example by cancelling a credit card or changing apassword?
  - If a large number of people are affected, or there are very serious consequences, you should inform the
    ICO.
  - Consider how notification can be made appropriate for particular groups of individuals, for example, if youare notifying children or vulnerable adults.
  - Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifyinga whole customer base of an issue affecting only one customer may well cause disproportionate enquiries and work.

  Clifton Homecare also need to consider who to notify, what to tell them and how to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to our decision:

  - Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notifythem of any type of breach but the ICO should only be notified when the breach involves personal data
  - There are a number of different ways to notify those affected so consider using the most appropriate one.
    Always bear in mind the security of the medium as well as the urgency of the situation
  - Your notification should at the very least include a description of how and when the breach occurred andwhat data was involved. Include details of what you have already done to respond to the risks posed bythe breach
  - When notifying individuals give specific and clear advice on the steps they can take to protect themselvesand also what you are willing to do to help them
  - Provide a way in which they can contact you for further information or to ask you questions about what hasoccurred – this could be a helpline number or a web page, for example.
  - When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform us if the media are aware of the breach so that we can manageany increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.

- The ICO has produced guidance for organisations on the information we expect to receive as part of a breachnotification and on what organisations can expect from us on receipt of their notification.

This guidance is available on their website here.

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank orcredit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review andupdate these policies and outline responsibility in the light of experience.
You may find that existing procedures could lead to another breach and you will need to identify whereimprovements can be made.

The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data securitybreach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do youstore data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method oftransmission is secure but also that you only share or disclose the minimum amount of data necessary.
  By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices oraccess to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and nontechnical staff who discuss 'what if'scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- If you have completed the Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches, or incorporating security breaches into the overallBusiness Continuity Plan. Breach of data security could in some circumstances be serious enough to endanger the business.
- It is recommended that at the very least you identify a group of people responsible for reacting to reportedbreaches of security.

GDPR01 – General Data Protection Regulations

Data Protection by design

Data protection by design is the process undertaken where data protection is considered and accounted for before new processes and systems are commenced. Prior to establishing new ways of working internally or externally data protection and security is explored. Only when assurances are provided and safe systems of working are concluded do new processes commence. An example of this in 2023 is the commencement of digital care planning and use of family portal for remote client and family login.

Note: All Policies are reviewed annually, more frequently, or as necessary.