1. **INTRODUCTION**

1.1 Unity Care Solutions is aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we hold on you as a Client of Unity Care Solutions. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

1. **DATA CONTROLLER DETAILS**
	1. Unity Care Solutions is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are UCS Head Office, 8a, The Old Oast House, Spelmonden Estate, Goudhurst, TN17 1HE.
2. **DATA PROTECTION PRINCIPLES**
	1. In relation to your personal data, we will:
* process it fairly, lawfully and in a clear, transparent way;
* collect your data only for reasons that we find proper for the service agreement with us in ways that have been explained to you;
* only use it in the way that we have told you about;
* ensure it is correct and up to date;
* keep your data for only as long as we need it;
* process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), nor lost or destroyed.
1. **TYPES OF DATA WE PROCESS**

4.1We hold many types of data about you, which could include:

* Your personal details including your name, address, date of birth, email address, phone numbers;
* Sometimes your photograph; sometimes a client specific training video
* Nationality & ethnicity
* Gender;
* Religion;
* Marital status;
* Dependants, next of kin and their contact numbers;
* Height, weight & BMI;
* Medical and health information including whether or not you have a disability;
* A ‘Do Not Resuscitate’ (DNR) directive
* A Mental Capacity Assessment (MCA)
* Risk assessments
* Building entry information;
* Financial transaction records;
* Personal profile information which may include your education, employment, pastimes and interests;
* Details of professionals involved in your care
* External professional guidelines
* Individual Placement agreements
* Bank details for invoicing;
* National Insurance number;
* National Health number;
* Client specific ID number;
* Complaints, concern forms, incident forms, safeguarding notifications
* Client feedback
* Compliments
1. **HOW WE COLLECT YOUR DATA**

5.1 We collect data about you in a variety of ways and this will usually start when we are asked to undertake to do an initial assessment of your needs and requirements where we will collect data as indicated in section 4.1 from the commissioning group and/or you directly.

5.2 Further information may be required from third party professionals such as GP, physios, occupational therapists etc. We would seek your consent before we undertake this.

1. **WHY WE PROCESS YOUR DATA**

6.1 The law on data protection allows us to process your data for certain reasons only:

* in order to provide your care;
* in order to carry out our legal requirements;
* in order for us to carry out our legitimate interests;
* to protect your interests; and where something is done in the public interest.

62 We also need to collect your data to ensure we are complying with legal requirements such as:

* making reasonable adjustments for disabled clients.
* complying with Care Quality Commission (CQC) regulations such as local authority safeguarding teams

6.3 We also collect data so that we can carry out activities which are in the legitimate interests of our organisation. We have set these out below:

* maintaining comprehensive up to date personnel records about you to ensure, amongst other things, continuity of care; effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained;
* effectively monitoring your needs and requirements to undertake procedures with regard to both of these as the need arises;
* complying with other regulatory bodies such as local authority safeguarding teams, CQC, DBS.
* offering a method of recourse for you via a complaints procedure;
* gaining expert medical opinion when making decisions about your wellbeing;
* dealing with legal claims made against us;
* preventing fraud;
* ensuring our administrative and IT systems are secure and robust against unauthorised access.
1. **SPECIAL CATEGORIES OF DATA**

7.1 Special categories of data are data relating to your:

* health;
* sex life;
* sexual orientation;
* race;
* ethnic origin;
* political opinion;
* religion;
* trade union membership;
* genetic and biometric data.

7.2 We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

* you have given explicit consent to the processing
* we must process the data in order to carry out our legal obligations
* we must process data for reasons of substantial public interest
* you have already made the data public.

7.3 We will use your special category data:

* for the purposes of equal opportunities monitoring;
* to determine reasonable adjustments.

7.4 We do not need your consent if we use special categories of personal data in order to carry out our legal obligations such as reporting a safeguarding incident or concern. However, we would inform you that it is our duty to do so.

7.5 We may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent. However, there may be repercussions if you choose to withhold consent as we may be prevented from providing aspects of your care and support.

1. **CRIMINAL CONVICTION DATA**

8.1 We will only collect criminal conviction data where it is appropriate where the law permits us. This data will usually be collected at the initial assessment stage. We use criminal conviction data in the following ways:

* As part of our safe ways of working for our staff when working with clients within the care sector.

8.2We process this data because of our legal obligation to undertake a safe environment for our employees working within the care sector.

1. **IF YOU DO NOT PROVIDE YOUR DATA TO US**
	1. One of the reasons for processing your data is to allow us to carry out our duties in line with your needs and requirements. If you do not provide us with the data needed to do this, we may be unable to perform those duties. We may also be prevented from confirming, or continuing with, your package of care with us.

**10. HOW WE STORE YOUR DATA**

10.1 Personal data is kept securely within locked filing cabinets in Unity Care Solutions offices which is

 locked when not in use by UCS office staff.

10.2 In the office, during office hours, visitors are kept away from working desks and computer screen locks

 are used.

10.3 In the office after working hours, staff operates a clear desk policy and data locked away. Computers

 are turned off. The office is locked.

10.4 Personal data is also stored on our IT systems which are password protected.

10.5 All computer records are protected with several layers of software to protect from cyber and virus

 attacks.

10.6 Account invoice details are stored on IT systems which are password protected.

10.7 Contact details are entered on a database and used to contact you by telephone, e-mail and post.

10.8 Contact details are also stored onto a password protected UCS mobile phone to enable our 24/7 on call

 facility.

10.9 Next of kin contact details and emergency information is also stored in paper format to enable our 24/7

 on call facility access if there is a wi-fi break in service. These are kept in lockable document

 security bags when out of office.

10.10 Your name is stated on staff rotas and your address and any entry codes details are sent to staff

 separately using your initials.

10.11 Staff are not permitted to store identifying client data on personal devises including mobile phones,

 iPad, lap tops, computers.

10.12 Working documents i.e. Medication Administration Records and daily logs being transferred between

 our office and you will be enclosed in sealed envelopes with our address on it and may be given to staff

 to deliver and/or return to the office at the earliest opportunity.

11. **SHARING YOUR DATA**

11.1 Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes our carers, our nurses, our care co-ordinators, our registered managers and our head office admin team.

11.2 We share some of your data with third parties in order to obtain further information on your health and medical needs. We would seek your consent before we undertake this.

11.3 We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

11.4 We do not share your data with bodies outside of the European Economic Area.

11.5 We may need to share your data with third parties as part of our legal obligations such as part of our

 Safeguarding procedures like local authority safeguarding teams, paramedics, police, CQC.

**12 PROTECTING YOUR DATA**

12.1 We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. Please refer to Unity Care Solutions’ Data Transfer Policy.

12.2 Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.Please refer to the GDPR guidance for third party holding shared data provided by UCS.

**13 HOW LONG WE KEEP YOUR DATA FOR?**

13.1 In line with data protection principles, we only keep your data for as long as we need it for, which is

 usually 8 years after of your package of care ceases for an adult service; or until a child reaches 26 years

 old after of your package of care ceases for a paediatric service user. However, we may need to keep some

 data that we are lawfully obliged to keep for Government agencies after your package of care has ended.

 You will be informed of this.

**14 DISPOSAL OF YOUR DATA**

14.1 In line with data protection principles, archived data is retained in a secure Data Storage facility at our head

 office.

14.2 Destroying of obsolete data is carried out by safely disposing of documents and/or media in authorised

 shredding receptacles (where there is no unauthorised access to the documents once deposited).

14. 3 We use a specialist data destruction specialist and use their vetted staff who collect obsolete data and

 media and shred in line with Data Protection Principles and BSEN:15713 Code of Practice.

14.4 We receive a ‘Certificate of Destruction’ from the company for our records.

**15 YOUR RIGHTS IN RELATION TO YOUR DATA**

15.1 The law on data protection gives you certain rights in relation to the data we hold on you. These are:

* the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice;
* the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request.
* the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it;
* the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it; however we may need to keep some data where we are lawfully obliged to keep for Government agencies after your package of care has ended.
* the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct;
* the right to portability. You may transfer the data that we hold on you for your own purposes;
* the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests;
* the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in a way that adversely affects your legal rights.

15.2 Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. However, there may be repercussions if you choose to withhold consent as we may be prevented from confirming or continuing with your package of care. In some cases, we may continue to use the data where we are lawfully obliged to keep for Government agencies.

16 National Data Opt-Out

Under the [national data opt-out](https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out) planned to be implemented by 31 July 2022, everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their “confidential patient information” with other organisations if it is not about managing or delivering their care. For example, if this information is used for research or planning purposes.

It does not affect how we share information with other organisations to manage someone’s care and it won’t apply if we have explicit consent to share information or if the information is appropriately anonymised.

As a care provider, we do not share confidential patient information except to manage or deliver care. The new opt-out should not have a major impact on our service users, but it is always important to treat people’s confidential information sensitively. So, if someone has opted out of sharing their data, we will not use confidential patient information for planning or research purposes, to ensure we comply with opt-out legislation.

We are using the term “confidential patient information” as this is the term already used by the NHS where the opt-out is already in force. “Confidential patient information” applies to information about someone’s health *or* social care that can identify them. <https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out>

**17 DATA PROTECTION OFFICER**

17.1 The Company’s Data Protection Officer is Maria Bolton (Managing Director). She can be contacted at mariabolton@unitycaresolutions.co.uk.

**18 MAKING A COMPLAINT**

18.1 If you wish to exercise any of the rights explained above, please contact Maria Bolton, Managing Director.

18.2 The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). ( If you think your data protection rights have been breached in any way by us, you are able to make a ccccccomplaint to the ICO:-

 Information Commissioner’s Office
 Wycliffe House
 Water Lane
 Wilmslow
 SK9 5AF

 Tel: 0303 123 1113 Email: <https://ico.org.uk/global/contact-us/email/>

|  |
| --- |
| ***Change and /or Review Record*** |
| **Issue Date** | ***Change*/Review** | ***Ratified by***  | ***Date*** |
| 29/08/2019 | *draft form* |  | *29/08/2018* |
| 29/05/2019 | *ratified* | *MB* | *29/05/2019* |
| 31/7/2022 | *updated with information of the National Opt out* | *DW* | *31/7/22* |
| 09/01/2023 | *review – no change* | *DW* | *09/01/23* |