CAREESSENCE
Caring for you holistically

GDPR POLICY AND KEY TERMS

GDPR Background

The General Data Protection Regulation will provide greater protection to individuals and place greater obligations on Careessence Limited (Careessence) to ensure that any impact on the provision of care and services is reduced to all staff and clients/service users. All Careessence staff are required to understand whether the ways in which they handle personal data already meet the requirements of GDPR and, if not, the steps that need to be taken to achieve compliance.

Our Approach to GDPR

Careessence is required to take proportionate and appropriate approach to GDPR compliance. Careessence understands that the approach to handling data privacy will depend on the volume and types of personal data processed, as well as the processes already in place to protect personal data.

Careessence understands that if significant volumes of personal data are processed, including special categories of data, or if there are unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.

GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

Careessence Limited's Process for Promoting Compliance

To ensure that Careessence understands and is able to comply with GDPR, all staff are required to review the following documents that will be produced over the next few months:

- Initial Privacy Impact Assessment Policy & Procedure
- GDPR – Key Terms Guidance
- GDPR - Key Principles Guidance
- GDPR - Processing Personal Data Guidance
- Appointing a Data Protection Officer Guidance (if necessary)
- Data Security and Retention Policy & Procedure
- Website Privacy Policy & Procedure
- Subject Access Requests Policy & Procedure
- Subject Access Requests Process Map Policy & Procedure
- Subject Access Requests - Request Letter Policy & Procedure
- Rights of a Data Subject Guidance
- Breach Notification Policy & Procedure
- Breach Notification Process Map Policy & Procedure
- Fair Processing Notice Policy & Procedure
- Consent Form
- GDPR - Transfer of Data Guidance

- Privacy Impact Assessment Policy & Procedure

Overview of Key Principles and Documents

The key principles and themes of each of the documents listed above are summarised below:

Initial Audit and Privacy Impact Assessment

Careessence Limited understands that we should conduct an audit of the personal data we currently process. This can be carried out internally by Careessence Limited with the assistance of key staff members. The audit will reveal whether the ways in which Careessence Limited processes personal data meet the requirements of GDPR and will also indicate whether Careessence Limited should delete some of the personal data it currently holds.

Key Terms

GDPR places obligations on Careessence regarding holding information on Data Subject. A brief description of those three key terms is included in the Definitions appendix of this document.

The requirements that Careessence Limited will need to meet will vary depending on whether Careessence Limited is a Data Controller or a Data Processor. We recognise that in most scenarios, Careessence Limited will be a Data Controller. The meaning of Data Controller and Data Processor, together with the roles they play under GDPR, will be explained in the Key Terms Guidance.

Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This will also be covered in more detail in the Key Terms Guidance.

Key Principles

There are 6 key principles of GDPR which Careessence Limited must comply with. These 6 principles are very similar to the key principles set out in the Data Protection Act 1998. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring the personal data is adequate and relevant
- Ensuring the personal data is accurate
- Ensuring the personal data is only retained for as long as it is needed
- Ensuring the personal data is kept safe and secure

These key principles will be explained in more detail in the guidance entitled 'GDPR – Key Principles'.

Careessence Limited recognises that in addition to complying with the key principles, Careessence Limited must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an after-thought. These ideas will also be covered in more detail in the Key Principles Guidance.

Processing Personal Data

The position has been improved under GDPR in terms of the ability of care sector Careessence to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories of data.

In terms of other types of personal data, Careessence Limited must only process personal data if it is able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are:

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the Data Subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above and the impact of the changes made in respect of special categories of data will be explained in more detail in the guidance entitled 'GDPR – Processing Personal Data'.

Data Protection Officers

Whether or not Careessence Limited needs to appoint a formal Data Protection Officer, Careessence Limited will appoint a single person to have overall responsibility for the management of personal data and compliance with GDPR.

Data Security and Retention

Two of the key principles of GDPR are data retention and data security.

- Data retention refers to the period for which Careessence Limited keeps the personal data that has been provided by a Data Subject. At a high level, Careessence Limited must only keep personal data for as long as it needs the personal data
- Data security requires Careessence Limited to put in place appropriate measures to keep data secure

These requirements will be described in more detail in the policy & procedure entitled Data Security and Retention, which will be drafted with a view to being circulated amongst staff at Careessence Limited.

Website Privacy Policy & Procedure

Where Careessence Limited collects personal data via a website, we understand that we will need a GDPR compliant website privacy policy. The privacy policy will explain how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy will be provided.

Subject Access Requests

One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where Careessence Limited receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of GDPR. To help staff at Careessence Limited understand what a Subject Access Request is and how they should deal with a Subject Access Request, a Subject Access Request Policy & Procedure will be made available to staff. A Careessence Limited process map to follow when responding to a Subject Access Request, as well as Subject Access Request letter template will also be included.

The Rights of a Data Subject

In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Careessence Limited. All rights of the Data Subject will be covered in detail in the corresponding guidance.

Breach Notification Under GDPR

We understand, that in certain circumstances, if Careessence Limited breaches GDPR, we must notify the ICO and potentially any affected Data Subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for Careessence Limited to follow if a breach of GDPR takes place will be published.

We understand that this requirement is likely to have less impact on NHS Careessence that are already used to reporting using the NHS reporting tool.

Fair Processing Notice and Consent Form

Careessence are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. The easiest way to provide that information is in a Fair Processing Notice. A Fair Processing Notice template will be produced for Careessence Limited to use and adapt on a case by case basis.

The Fair Processing Notice will sit alongside a consent form which can be used to ensure that Careessence Limited obtains appropriate consent, particularly from the Service User, to the various ways in which Careessence Limited uses the personal data. The Consent Form will contain advice and additional steps to take if the Service User is a child or lacks capacity.

Transfer of Data

If Careessence Limited wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for

example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance will be produced to explain the implications of transferring personal data in more detail.

Privacy Impact Assessments

In addition to carrying out an Initial Impact Assessment (referred to above), Careessence Limited will carry out further assessments each time it processes personal data in a way that presents a “high risk” for the Data Subject. Examples of when a Privacy Impact Assessment should be conducted will be provided in the relevant policy & procedure. Given the volume of special categories of data that are frequently processed by Careessence in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed.

The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

Compliance with GDPR

Careessence Limited understands that there are two primary reasons to ensure that compliance with GDPR is achieved:

- It will promote high standards of practice and care, and provide significant benefits for staff and, in particular, Service Users
- Compliance with GDPR is overseen in the UK by the ICO. Under the Data Protection Act 1998, the ICO has the power to levy fines of up to £500,000 for the most serious breach. Under GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences are therefore significant.

Careessence Limited appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants Careessence to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if Careessence Limited persistently breaches GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of

special categories of data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Careessence Limited and our data protection policies and processes Careessence

Limited realises that the ICO may also require Careessence Limited to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

Appendix 1 – Key terms

When does GDPR apply?
GDPR applies to any organisation that processes personal data relating to a data subject.

Does the GDPR Apply to you?
If you process personal data within the EU, GDPR will apply. It applies to all organisations including, for example, public authorities, not for profit organisations, limited companies, trusts, charities and sole traders. GDPR does not apply to individuals using information in their personal capacity. For example, if you store a notebook of phone numbers of your friends and family in your filing cabinet at home, this will not be captured by GDPR.

What is Personal Data?
Personal data is any information that relates to a living individual. It does not include personal information about somebody who has died.

The definition of personal data is wider under GDPR than under the Data Protection Act and includes specific identifiers, such as a person's name and email address, as well as factors about a person, such as their physical appearance, physiological or mental state, their financial status or social identity. It could, therefore, include opinions you give about a person in their care records or care plan, and will certainly include a person's medical and health records. The definition also includes photographs and CCTV footage, as well as location data.

Personal data includes business contact information of an individual, i.e. an individual's business email address such a joe.bloggs@careagency.com. It does not include generic business email addresses such as info@careagency.com or any other general business information.

Although GDPR does not distinguish between "personal" personal data (e.g. joe.bloggs@gmail.com) and "business" personal data (e.g. joe.bloggs@careagency.com), the Information Commissioner's Office (the body that oversees compliance with GDPR) is likely to be more concerned about unauthorised loss or disclosure of "personal" personal data.

"Special categories of data" are a type of personal data, and have broadly the same meaning as "sensitive personal data" under the Data Protection Act. They include types of data that are thought to be of a more sensitive nature, such as information about a person's medical history or health, their race or ethnic origin, their religious or political views and their sexual orientation. The definition also includes genetic data and biometric data.

Under GDPR, organisations are not entitled to process Special Categories of Data unless one of the 10 exceptions applies. One of the exceptions expressly refers to processing that is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnoses, the provision of health or social care or treatment or the management of health or social care systems and services. Special Categories of Data can, therefore, be processed without consent for those purposes. This will be considered in more detail in the guidance note that explains the requirements around processing personal data.

What do you Need to do with Personal Data for GDPR to Apply?
In practice, anything. At the point you collect personal data, you are processing it. You don't need to be doing anything actively with the data – just holding or storing it (even if you never look at it) means that you are processing it.

Other activities that constitute processing may include (but aren't limited to) adapting or modifying the personal data, deleting, copying, organising, retrieving and transferring it.

Does GDPR Apply to all Personal Data, Irrespective of where it is Stored?
GDPR only applies to personal data stored in a filing system. The majority of personal data held on computers or online will be held in a filing system because even if the document has been stored incorrectly, it's likely it could still be retrieved using a search function.

If paper files are stored in a logical order (chronologically or alphabetically, for example), they will also be captured by GDPR. If you throw paper documents into a disorganised confidential waste bin, for example, GDPR will no longer apply to the personal data within those documents.

Who is the Data Subject?

The data subject is the living individual whose personal data is being processed by an organisation

What about the Data Controller and the Data Processor?

The data controller is the organisation that determines the purposes and means for which the personal data is processed.

For example, at the point a care home is passed the personal data of a service user, the care home will decide how to use that data – for example, it will use medical records to understand which medicines need to be administered and to understand behavioural issues, and it will use phone numbers for next of kin to contact them in the event of an emergency.

If an organisation wants or needs a third party to do something with the personal data, at the point the personal data is passed to the third party, the third party becomes a data processor. The data processor only uses the personal data in accordance with instructions given by the data controller. For example, if an organisation outsources its HR or payroll function, the HR or payroll provider will be data processor of the personal data passed to it to administer HR or payroll services.

In most situations, care homes and agencies and similar organisations will be data controllers of the personal data they process.

Last update 18 04 10