Overarching GDPR Policy and Procedure

1. Policy

1.1 GDPR Background

GDPR will come into force on 25 May 2018 and will replace the Data Protection Act 1998. GDPR will be implemented regardless of Brexit. GDPR will provide greater protection to individuals and place greater obligations on organisations, but it can be dealt with in bite-size chunks to ensure that any impact on the provision of care and services is reduced.

1.2 All staff will need 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.

1.3 Courage Healthcare Ltd.'s Approach to GDPR

Courage Healthcare Ltd is required to take a proportionate and appropriate approach to GDPR compliance. Courage Healthcare Ltd understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. We understand that if we process significant volumes of personal data, including **special categories of data**, or have 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.

1.4 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.

1.5 Courage Healthcare Ltd.'s Process for Promoting Compliance

To ensure that Courage Healthcare Ltd understands and is able to comply with GDPR, all staff should review the following documents that will be produced over the next few months:

1.5.1 Initial Privacy Impact Assessment Policy & Procedure
1.5.2 GDPR – Key Terms Guidance
1.5.3 GDPR - Key Principles Guidance
1.5.4 GDPR - Processing Personal Data Guidance
1.5.5 Appointing a Data Protection Officer Guidance
1.5.6 Data Security and Retention Policy & Procedure
1.5.7 Website Privacy Policy & Procedure
1.5.8 Subject Access Requests Policy & Procedure
1.5.9 Subject Access Requests Process Map Policy & Procedure
1.5.10 Subject Access Requests - Request Letter Policy & Procedure
1.5.11 Rights of a Data Subject Guidance
1.5.12 Breach Notification Policy & Procedure
1.5.13 Breach Notification Process Map Policy & Procedure
1.5.14 Fair Processing Notice Policy & Procedure
1.5.15 Consent Form
1.5.16 GDPR - Transfer of Data Guidance
1.5.17 Privacy Impact Assessment Policy & Procedure

1.6 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

Courage Healthcare Ltd understands that we should conduct an audit of the personal data we currently process. This can be carried out internally by Courage Healthcare Ltd with the assistance of key staff members. The audit will reveal whether the ways in which Courage Healthcare Ltd processes personal data meet the requirements of GDPR and will also indicate whether Courage Healthcare Ltd should delete some of the personal data it currently holds. An initial Privacy Impact Assessment template will be provided as part of the GDPR documentation.

Key Terms

GDPR places obligations on all organisations that process personal data about a Data Subject. A brief

description of those three key terms is included in the Definitions section of this document and will be expanded upon in the Key Terms Guidance.

The requirements that Courage Healthcare Ltd will need to meet will vary depending on whether Courage Healthcare Ltd is a Data Controller or a Data Processor. We recognise that in most scenarios, Courage Healthcare Ltd 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 Courage Healthcare Ltd must comply with. These 6 principles are very similar to the key principles set out in the Data Protection Act 1998. They are:

1.6.1 Lawful, fair and transparent use of personal data
1.6.2 Using personal data for the purpose for which it was collected
1.6.3 Ensuring the personal data is adequate and relevant
1.6.4 Ensuring the personal data is accurate
1.6.5 Ensuring the personal data is only retained for as long as it is needed
1.6.6 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'.

Courage Healthcare Ltd recognises that in addition to complying with the key principles, Courage Healthcare Ltd 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 organisations 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, Courage Healthcare Ltd 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:

1.6.7 The Data Subject has given his or her consent to the organisation using and processing their personal data
1.6.8 The organisation is required to process the personal data to perform a contract; and
1.6.9 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:

1.6.10 The processing is necessary to comply with a legal obligation
1.6.11 The processing is necessary to protect the vital interests of the Data Subject or another living person
1.6.12 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

Courage Healthcare Ltd understands that some organisations will need to appoint a formal Data Protection Officer under GDPR (a "**DPO**"). The DPO benefits from enhanced employment rights and must meet certain criteria, so we recognise that it is important to know whether Courage Healthcare Ltd requires a DPO. This requirement will be outlined in the policy and procedure on Data Protection Officers.

Whether or not Courage Healthcare Ltd needs to appoint a formal Data Protection Officer, Courage Healthcare Ltd 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.

1.6.13 Data retention refers to the period for which Courage Healthcare Ltd keeps the personal data that has been provided by a Data Subject. At a high level, Courage Healthcare Ltd must only keep personal data for as long as it needs the personal data

1.6.14 Data security requires Courage Healthcare Ltd 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 Courage Healthcare Ltd.

Website Privacy Policy & Procedure

Where Courage Healthcare Ltd 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 Courage Healthcare Ltd 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 Courage Healthcare Ltd 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 Courage Healthcare Ltd process map to follow when responding to a Subject Access Request, as well as a 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 Courage Healthcare Ltd. 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 Courage Healthcare Ltd 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 Courage Healthcare Ltd to follow if a breach of GDPR takes place will be published.

Fair Processing Notice and Consent Form

Organisations 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 Courage Healthcare Ltd 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 Courage Healthcare Ltd obtains appropriate consent, particularly from the Service User, to the various ways in which Courage Healthcare Ltd 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 Courage Healthcare Ltd 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), Courage Healthcare Ltd 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 organisations 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'.

1.7 Compliance with GDPR

Courage Healthcare Ltd understands that there are two primary reasons to ensure that compliance with GDPR is achieved:

1.7.1 It will promote high standards of practice and care, and provide significant benefits for staff and, in particular, Service Users

1.7.2 Compliance with GDPR is overseen in the UK by the ICO.

Courage Healthcare Ltd 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 organisations to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if Courage Healthcare Ltd 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 Courage Healthcare Ltd and our data protection policies and processes Courage Healthcare Ltd realises that the ICO may also require Courage Healthcare Ltd to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

2. Procedure

2.1 All staff should review the GDPR policies and procedures and guidance that will be produced over the next few months.

2.2 Courage Healthcare (West Midlands) Ltd will nominate a person or team to be responsible for data protection and GDPR compliance (if a formal Data Protection Officer is not required, somebody with an understanding of the requirements who can act as a day-to-day point of contact will be chosen).

2.3 Registered Manager should ensure all staff understand the policies and procedures provided, including how to deal with a Subject Access Request and what to do if a member of staff breaches GDPR.

2.4 Registered Manager will consider providing training internally about GDPR (in particular, the Key Principles of GDPR) to all staff members.

2.5 Courage Healthcare Ltd will conduct an audit of the personal data currently held by Courage Healthcare Ltd (the initial Privacy Impact Assessment template provided will be used for this purpose).

2.6 Courage Healthcare Ltd will delete any personal data that Courage Healthcare Ltd no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice for Health and Social Care 2016.

2.7 Courage Healthcare Ltd will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with GDPR.

2.8 Courage Healthcare Ltd will, if necessary, finalise and circulate a Fair Processing Notice to Service Users.

2.9 Courage Healthcare Ltd will ensure proper consent is obtained from each Service User in line with

GDPR regulations (the Consent Form provided can be used for this purpose). Courage Healthcare Ltd will review the additional steps that Courage Healthcare Ltd should be taken to ensure that Courage Healthcare Ltd obtains consent from parents, guardians, carers or other representatives where Courage Healthcare Ltd works with children or those who lack capacity.

2.10 Courage Healthcare Ltd will ensure that processes and procedures are in place to respond to requests made by Data Subjects (including Subject Access Requests) and to deal appropriately with any breaches or potential breaches of GDPR.

2.11 Registered Manager will maintain a log of decisions taken and incidents that occur in respect of the personal data processed by Courage Healthcare Ltd using the Courage Healthcare Ltd Privacy Impact Assessment template.

3.1 Data Subject

The individual about whom Courage Healthcare Ltd has collected personal data

3.2 Data Protection Act 1998 The law that relates to data protection. It will remain in force until and including 24 May 2018. It will be replaced by GDPR on 25 May 2018

3.3 GDPR

The General Data Protection Regulation 2016. It will replace the Data Protection Act 1998 from 25 May 2018 as the law that governs data protection in the UK. It will come into force in the UK via the Data Protection Bill

3.4 Personal Data

Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, defined below

3.5 Process or Processing

Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

3.6 Special Categories of Data

Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 1998. Special Categories of Data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views

Key Facts -Professionals

Professionals providing this service should be aware of the following:

- GPDR provides greater protection for staff and Service Users in respect of their personal data
- Compliance is mandatory, not optional
- Courage Healthcare Ltd will adopt an appropriate and proportionate approach what is right and necessary for Courage Healthcare Ltd may not be right for another organisation
- Achieving compliance with GDPR will not only reduce the risk of ICO enforcement or fines but will also promote a better-quality service for Service Users and an improved working environment for staff