Information Governance and wider GDPR Agreement between Clinical Transparency Ltd and individual practices / clinics.

Clinical Transparency Ltd provides an online, cloud-based, encrypted tool (Care Response) which assists in the collection and collation of Patient Reported Outcome Measures (PROMs), Patient Reported Experience Measures (PREMs) and other data collected from questionnaires.

It provides analyses of patient and practice level data in order to provide information on individual patients progress. This can be used to improve the patient centeredness of care and to assist with shared decision making as well as providing internal intelligence on care standards and productivity for clinics.

This document sets out the Information Governance (IG) and data protection arrangements that surround the analysis service provided by Clinical Transparency Ltd, in line with the GDPR. It identifies the role of each clinic as the overarching Data Controller and defines the role of Clinical Transparency Ltd as the Data Processor. Furthermore, this agreement determines the responsibilities and duties of both Data Controller and Data Processor.

Each clinic utilising the analytical tool provided by Clinical Transparency Ltd is asked to read this document fully, and to signal their comprehension and agreement with the information contained within by signing and dating the document on page 5.

Overview

- Organisations using care response are responsible for setting patients up on the system having gained their consent to do this.
- Organisations using care response will have their own IG policies and procedures ensuring their compliance with relevant data protection legislation including GDPR. Their use of Care Response or other services supplied by Clinical Transparency Ltd will be subject to these.
- Clinical Transparency Ltd will be the 'data processor' and will only manipulate data and will not use the data from patients / clinics / practices in any way without the explicit consent of the patient / clinic / practice.
- Clinical Transparency Ltd will take all reasonable steps to maintain, process and transmit the data in a secure fashion. This includes making regular backups and ensuring both physical and electronic security measures. Routine risk assessment and information security audits will be undertaken and documented.

1. Introduction

The GDPR sets out seven key principles (See Annex 1):

2. Lawfulness, fairness and transparency
3. Purpose limitation
4. Data minimisation
5. Accuracy
6. Storage limitation
7. Integrity and confidentiality (security)
8. Accountability

These principles give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

In data protection terms, these organisations must act as either Data Controllers or Data Processors.

This agreement sets out the role of the Data Controller and the Data Processor, what their roles and responsibilities are, and the governance issues that have to be addressed to ensure GDPR compliance.

9. The Data Controller

The Data Controller is the organisation (clinic or practice) who initially gathers and collates data. The Data Controller determines the purposes for which, and the way in which, personal data is processed.

2.a Responsibilities of the Data Controller

- Collects personal or sensitive information direct from source, and holds a legal basis for doing so.

- Determines which items of personal data to collect.

- Identifies the purpose(s) the data are to be used for.

- Determines which individuals to collect data about.

- Obtains explicit consent from the data subject (i.e. patient) for the collection and processing of their information, and provides the data subject with information as to how they can withdraw this consent at any time.

- Provides specific information to the data subject; i.e. the organisation's identity, details of the personal data you hold about the data subject, and what this information will be used for.

- Complies with GDPR principles as set out in Annex 1.

May 2018, V2.1

- Determines whether to disclose the data, and if so, why and to whom.
- Determines how to respond to any Freedom of Information access requests, and manages these responses.
- Agrees how long to retain the data, and / or whether to make non-routine amendments to the data.
- Implements technical and organisational measures to protect personal data against accidental loss/destruction, unauthorised access or other unlawful processing.
- Agrees with the Data Processor what is to happen with previously provided data when a data processing agreement is terminated.
- Exercises overall control over the purpose for which, and the manner in which, personal data are processed.
- Holds data protection responsibility for the data at all times.

The Data Controller can contractually or informally agree to utilise a Data Processor to process their data for analytical or reporting purposes. Within this agreement, the Data Processor is Clinical Transparency Ltd.

10. The Data Processor

The Data Processor is the organisation who processes data on behalf of the Data Controller. As previously stated, Clinical Transparency Ltd operates as a Data Processor.

3.a Responsibilities of the Data Processor

- To process the data on behalf of the Data Controller, as requested by the Data Controller.

> **"Processing",** in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
>
> a) Organisation, adaption or alteration of the information or data
>
> b) Retrieval, consultation or use of the information or data
>
> c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
>
> d) Alignment, combination, blocking, erasure or destruction of the information or data.

- To identify the most appropriate data collection and analysis tool for the agreed processing purpose.
- To maintain a record for all processing operations under their responsibility.
- To ensure that all data provided is stored securely.

May 2018, V2.1

- To ensure that all data transmitted is done so securely and appropriately, and to recognize their direct responsibility for ensuring appropriate security measures are in place.

- To ensure that there are appropriate means for retrieving personal information about individual patients.

- To ensure that there are means to delete or dispose of data, should this be requested by the Data Controller.

- To ensure that data is only analysed in such a way that is requested / agreed with the Data Controller.

- To ensure that data is not shared inappropriately, and to inform the Data Controller immediately of any data breach.

- To have a named Data Protection Officer in place.

11. Freedom of Information Access Requests

Requests can be made by public and private organisations or by unique individuals to ascertain access to shared data. Such a request may be received by either the Data Controller (the individual clinic or practice) or by the Data Processor (Clinical Transparency Ltd).

Whilst both organisations are to work together to respond to the access request, it is the role of the Data Controller to lead the provision of a response, and to ultimately decide whether access to the information requested is to be granted.

12. Audit and Quality Assurance

Both Data Controller and Data Processor are responsible for ensuring that data shared between these two parties is accurate.

Data Controllers should instigate periodic sampling to ensure that the data provided to the Data Processor accurately reflects the raw information gathered.

Data Processors should alert the Data Controller to any instances of incompatible data sets being provided to them, or of any data that has been recorded in an incorrect way.

Both Data Controllers and Data Processors have a responsibility to ensure the security of all information assets; and to prepare written assurance / evidence of the completion of relevant risk assessments and asset security audits.

13. Signature of Agreement

Signature:	Signature:
Print name:	Print name:
On Behalf of:	On Behalf of: Clinical Transparency Ltd
Date:	Date:
Email address:	

Sign, data and print name of individual and organisation above. Send copy of completed form to jfield@care-response.com and it will be countersigned and returned to you at the email address you provide above.

May 2018, V2.1

Annex 1: The GDPR Principles

1. Principle (a): Lawfulness, fairness and transparency

You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.

You must ensure that you do not do anything with the data in breach of any other laws.

You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

You must be clear, open and honest with people from the start about how you will use their personal data.

2. Principle (b): Purpose limitation

You must be clear about what your purposes for processing are from the start.

You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.

You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

3. Principle (c): Data minimisation

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;

- relevant – has a rational link to that purpose; and

- limited to what is necessary – you do not hold more than you need for that purpose.

4. Principle (d): Accuracy

You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.

You may need to keep the personal data updated, although this will depend on what you are using it for.

If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.

You must carefully consider any challenges to the accuracy of personal data.

5. Principle (e): Storage limitation

You must not keep personal data for longer than you need it.

You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.

You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.

You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.

You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.

You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

6. Principle (f): Integrity and confidentiality

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

7. Principle (g): Accountability principle

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance.