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

February 2017, V1.1

Clinical Transparency Ltd provides an online, cloud-based, encrypted tool (Care Response) which analyses patient and practice level data in order to provide internal intelligence on care standards and productivity for clinics. Outcome analysis from the Clinical Transparency Ltd software can also be used by clinics to populate Patient Reported Outcome Measures (PROMs), Patient Reported Experience Measures (PREMs) and other data collected from questionnaires.

This document sets out the Information Governance (IG) arrangements that surround the analysis service provided by Clinical Transparency Ltd. 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 3.

Overview

- Organisations using care response are responsible for setting patients up on the system having gained their permission to do this.
- Data entered by organisations, practice or patients is 'owned' by these organisations/ practices and can not be used for any purpose without their consent.
- Patients have the right to see any data held about themselves subject to information governance rules in local territories.
- Clinical Transparency Ltd will be the 'data processor' and will only manipulate and will not use the date from patients / organisations in any way without the consent of the organisations.
- 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.

1. Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling (*see Annex 1*). These 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 data protection compliance.

2. The Data Controller

The Data Controller is the organisation (clinic or practice) who initially gathers and collates data. It is the Data Controller who owns the data. Within this agreement, the Data Controller is the individual clinic or practice.

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.

- Determines whether to disclose the data, and if so, why and to whom.

- Determines how to respond to any DPA or 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.

- 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.

3. 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 ensure that all data provided is stored securely.

- To ensure that all data transmitted is done so securely and appropriately.

- To ensure that there are appropriate means for retrieving personal information about certain individuals, if this level of data is provided initially by the Data Controller.

- 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.

4. DPA or 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.

5. 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.

6. Signature of Agreement

On Behalf of

On Behalf of Clinical Transparency Ltd

Annex 1: The Data Protection Principles

1. "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-(a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".

2. "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

3. "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

4. "Personal data shall be accurate and, where necessary, kept up to date".

5. "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

6. "Personal data shall be processed in accordance with the rights of data subjects under this Act".

7. "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

8. "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".