Information Governance and Data Protection Policy

Distribution: Staff, Clinical Partners, Clients on request
Date of issue: September 2014
Review date: January 2018
Next Review: July 2019

Author - Barny Guthrie, CEO

Clinical Partners
It's about getting better

Contents

Information Governance and Data Protection Policy

1. Introduction

Clinical Partners Ltd. (the Company) recognises the importance of reliable information and the contribution it makes to the objective of the company which is to provide access to the highest quality mental health outpatient care. Clinical Partners is committed to operating robust arrangements for information governance to ensure that its uses data in a secure and effective way. The organisation is always mindful of the clients right to be assured of confidentiality and in a way that seeks always to minimise the risk of loss or misuse of personal identifiable data.

The Board of Clinical Partners recognises its responsibilities under the Data Protection Act and from May 2018 the GDPR, to maintain the security and confidentiality of all person identifiable data that it handles and has developed procedures to ensure that this occurs. Clinical Partners seeks to work in a transparent and accountable manner when handling information relating to individuals.

2. Purpose and Principles of Data Protection

The Information Governance (IG) Policy sets out the how the Company will ensure that information is used effectively, efficiently, securely and legally, and the steps that it will take to minimise loss/breach of confidential data that it manages. The principles of GDPR are based on accountability. The organisation will ensure that all information relates to the following principles:

- It is lawful, fair and transparent
- It is collected and retained for a specific purpose
- The information is relevant and accurate
- Information is held securely
- Individuals' rights are observed

3. Scope

This policy covers the use and management of information in all formats, (e.g. paper, electronic) including the security, availability, collection, processing, storage, communication and disposal of information.

The introduction of GDPR 2018 applies across the whole of the EU and affects any non- EU business offering services to EU citizens.

The policy applies to all employees and contractors working for or supplying services to or for the Company.

4. Definitions

The following terms will be used in this policy:

Information Governance – Relates to the way the organisation processes or handles information in a legal and secure manner.

Personal Data – Information held by the organisation on individuals accessing their services

Data Subject – This is an individual who can be identified from information recorded about them and to whom the information relates

Data Controller – This is how the organisation controls and manages the information they hold

Data Processor – This is a third-party organisation that manages, processes and stores data on behalf of the organisation. An example would be outsourced payroll.

Under GDPR there are new responsibilities for Processors which will include the Data Controller ensuring the Processor is complaint with GDPR in terms of diligence and data protection and if necessary auditing their processes.

5. GDPR – What is changing?

In May 2018 GDPR is becoming the law and will affect all European Countries or those countries who provide services to European citizens. The changes will affect:

- Consent
- Scope
- Accountability
- Children
- Rights
- Processors
- Breaches
- Fines

Consent

This involves organisations having clear messaging and a positive opt – in tick box rather than an assumption of opt in. Consent for information must be recorded without detriment and an individual can withdraw consent at any time.

Scope

As above

Accountability

The organisation must demonstrate compliance and record all processing activities. All actions should be documented both by the Data Controller and Processor.

Children

All communication with children must have child friendly messaging. There must be Guardian consent where applicable with age verification.

Rights

This relates to the individual's right to be informed and have access requests. Individuals will have the right to have data erased (unless required by law) and the right to move or transfer data. No charges can be levied for providing personal data to that individual.

Data Processors

The Data Controller must ensure that any Data Processor is complaint with GDPR and this should be documented in any contractual agreement or terms along with specific responsibilities. Under GDPR there are new responsibilities for Processors.

The Data Processor must carry out GDPR diligence and data protection. The following should be considered when reviewing the lawfulness of processing:

- Data Subject has given consent
- It is required for performance of a contract
- Legal obligation
- To protect interests of the Data Subject
- It is in the public interest
- It is a legitimate interest of the Data Controller

Breaches and Fines

Any breaches need to be notified to the data subject and recorded as a minimum. There needs to be a notification to the regulatory body. Examples of notification requirement are accidental deletion or a lack of privacy where an individual's data has been deliberately or otherwise seen by an unauthorised individual. Other breaches include errors in Data retention and Processing.

Fines for any breach can be up to 4% of global turnover or 20m Euros.

6. Duties and Responsibilities

Chief Executive Officer

The CEO has ultimate responsibility for all elements of governance, including information governance within the Company. The CEO will work with staff and the Governance and Risk Adviser, together with externally contracted experts to ensure that Clinical Partners takes all reasonable steps to develop and implement systems and processes that effectively protect confidential data about patients, staff and clinicians engaged by the Company.

Data Protection Officer

The Governance and Risk Advisor is the Data Protection Officer and where necessary seeks guidance from experts in Data Protection to ensure compliance with GDPR. As part of the compliance process there should be a programme of audit of data systems and policies.

This policy documents Clinical Partners approach to Data Protection and this provides internal guidance for staff. New staff will receive training in their Induction regarding compliance and Data Protection.

All Staff and Clinicians supplying clinical services via the Company

All staff working for the company and Partners engaged to provide patient services via the Company must work within this policy by remaining vigilant to information risks; actively risk assessing elements that they are responsible for, and for identifying and escalating any risks that are (via assessment or because of an incident) outside of their control to allow mitigation to an acceptable level.

7. Procedures for Maintaining Effective Information Governance

7.1 Meeting Legal Compliance

- The Company is registered for holding personal data as required under the Data Protection Act 1998 and more recently GDPR 2018. Requirements for legal compliance are referred to above.

- The Privacy Policy for Clinical Partners has been reviewed and rewritten considering the GDPR changes 2018. This can be accessed on the Clinical Partners website and all prospective users of Clinical Partners services are encouraged to read the Privacy policy and accept its terms.

- All clinical staff and Clinical Partner employees have been informed of the data changes made by Clinical Partners in relation to the GDPR and how they may change, if at all, the way we communicate with clients.

- The Company will ensure Digital compliance by undertaking regular analysis of data, documenting and actioning system changes.

- Where Data Processors are involved the Company will ensure compliance through audit and contractual terms.

- The Company regards all identifiable personal information relating to clients, partners, staff and contractors as confidential, and will ensure data is held in secure ways (e.g. locked filing cabinets for paper data and on secure servers (not on hard drives) of company computers)

- When data subject identifiable data is held by the company this will be treated as confidential and will only accessed on a 'needs to know basis' for the delivery of the services of the company or to undertake administrative processes necessary for the delivery of those services

- The Company will fully cooperate with any official audit[1] of its practices in relation to information security if required to by statutory agencies and/or purchasers of the Company's services

[1] In the case of an official audit e.g.

- The Company regards all identifiable personal information relating to staff/ contractors as confidential except where national policy on accountability and openness requires otherwise or where required for fraud investigation.

- Data subjects, for whom data is recorded, or held in paper format by the Company are entitled, in law, to request details of information held about them, have the information erased or transferred. The Company must respond under arrangements in the Data Protection Act and GDPR 2018.

7.2 Information Security

The Company will maintain effective security arrangements for the access to and management of confidential information through

- Full HR checks prior to appointment of staff to the Company.

- Privacy Policy for employees outlining the use and retention of their data by the Company

- a requirement for all staff and contracted clinicians working for the Company to be issued with and accept in writing a statement of personal responsibility in relation to confidentiality.

- rigid enforcement of systems for the use of individual access passwords to all electronic data/materials held by the Company, with disciplinary action / loss of contractual rights (Clinical Partners) being taken in the event of a wilful breach of data security.

- Clinical Partners uses an industry standard data management product Clinic Office version 5[2] which provides industry level security of personal information

- All records will be held electronically on an externally hosted web accessed, password controlled server, and no paper records will be made of personal details /financial details of our patients.

- Financial management of patients invoices is handed via an externally hosted web based secure provider; 'Card safe'[3], which is a division of World Pay

- When paper records are held e.g. complaints correspondence this will always be held in a locked filing cabinet and access will be limited on a 'needs to know' basis

- The Company will ensure all Data Processors used by them are compliant to GDPR 2018 through compliance audits.

7.3 Responding to data related incidents

If an actual or potential breach of confidential information occurs the person identifying the incident must report it to the CEO via the Incident Reporting Procedure. The CEO will then be responsible for investigation and will call on experts as required to assist this investigation.

In the unlikely event that the Company suffers a security breach (data loss through theft, hacking or other means) the CEO will report the breach to the I Information Commissioner as required under the Data Protection and GDPR 2018.

---

by the Information Commissioner full cooperation will always be given. In the event of a potential supplier wishing to conduct their own Information Govern ace Audit this will be limited to an audit of systems and processes and no confidential data (data subject or financial data) will be subject external inspection

[2] http://www.pioneersoftware.co.uk/

[3] http://www.cardsave.net

Any data subject, or person properly authorised by the data subject may request copies of any personal data held about them, and this will be supplied on receipt of the appropriate written request. Clinical Partners will respond to any written request for disclosure of personal data in accordance with GDPR 2018.

Any data subject, or person authorised by the data subject may request copies of any personal data held about them and this will be supplied. Since GDPR 2018 no fee will be required.
The only exceptions to supplying documents is if the holder of the record believes that disclosure could do harm to the individual or another person. In the case of dispute about disclosure the company will seek legal advice.

Any client seeking access to clinical records will be asked to direct their request in writing to their clinician who will be responsible for responding to the request.

8. Process for maintaining confidentiality under the requirements of the Data Protection Act 1998 and GDPR 2018

8.1 Data Security and Disclosure

All staff /contractors working for the Company are responsible for ensuring that:

- They avoid holding person identifiable data as far as possible
- Any personal data which they hold is kept securely either electronically in a password protected system or in a locked cabinet
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party,
- That they will take all reasonable efforts to ensure data is not disclosed accidentally.

8.2 Retention of data

As the Company is concerned with the delivery of clinical services the Company will adopt data retention recommendations set out by the Department of Health, in accord with advisory times required to deal with legal disclosure

- Person identifiable data held on clients will be held for a minimum of 8 years following the last contact (or lifetime in relation to cases related to adoption).
- Person identifiable data on staff (e.g. related to employment etc.) 5 years from termination of employment
- Person identifiable information on clinician's engaged to provide services via contract (clinical partners) 21 years from the end of the contractual arrangement (in light of the clinical work being in mental health, the recommended retention period for m all mental health records is 21 years)
- Person identifiable information on potential contractors/contractors professional information to be held for as long as there is a professional relationship between person/organisation and the Company. If a contractual agreement is entered into the information will be retained for 8 years after the conclusion of business.
- Where data relates to adoption cases, client information needs to be kept for a lifetime. Clinicians are asked to send client records, via recorded delivery, to Clinical Partners Head Office as and when they stop working with Clinical Partners.

9. Process for Monitoring Compliance with this policy

9.1 When considering compliance, the following need to be considered:

- Users Rights
- Security
- Training
- Policies
- Review

9.2 A rolling programme of audits will be established to ensure the robustness of local systems for the storage and access of confidential data. Results of these audits and any action plans will be included in the CEO's report to the Board

9.3 In the event there is an actual breach of confidentiality the CEO will report on the results of the investigation (if any) and the steps taken to minimise risk of recurrence. The effect of any changes will be monitored by analysis/ audits.

9.4 Effectively managing GDPR compliance will install trust and confidence in Clinical Partners clients and future clients.

9.5 Managing compliance will start with:

- Single point of contact – Data Protection Officer
- Audit data, systems and policies
- Document approach to data protection and ensure policies are in place
- Internal documentation and guidance for staff
- Training staff
- Maintain compliance and keep up to date

10. Related Policies and Procedures and references

- Clinical Partners Risk Management Strategy and Policy
- GDPR 2018
- Information Commissioners web site http://ico.org.uk/
- Incident Reporting Policy