Clinical Partners
It's about getting better

INFORMATION GOVERNANCE AND DATA PROTECTION POLICY

Author: Barny Guthrie - CEO

Issued: September 2014
Review: July 2017
Next Review: July 2019

Distribution: Staff, Clinical Partners, Clients on request

Contents

Policy and Procedure for
Information Governance and Data Protection

1 Introduction

Clinical Partners Ltd. (the Company) recognises the vital contribution that reliable information makes to achievement of the objective of the company to provide access to the highest quality mental health outpatient care. It is committed to operating robust arrangements for information governance to ensure that its uses data in a safe an effective way, 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 to maintain the security and confidentiality of all person identifiable data that it handles and has developed procedures to ensure that this occurs.

2 Purpose

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.

3 Scope

This policy and associated procedures 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 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:

Term	Definition
Information Governance	**Relates** to the way organisations 'process' or handle information. **covers** personal information, relating to service users and employees, and corporate information, e.g. financial information **provides** a way for staff and contractors to deal consistently with the many different rules about how information is handled, including those set out in: • The Data Protection Act 1998

	• The Freedom of Information Act 2000 • The common law duty of confidentiality
Data Subject	An individual who can be **identified** from information recorded about then and to whom that information relates.
Access to data held by the Company	A data subject can ask to access any information held about them by the Company under the provisions of the Data Protection Act. The only exceptions to disclosure are if the Data Controller believes that disclosure of the data could lead to harm to the data subject or another person. In practice all data should be held in the expectation that the data subject may wish to access it.

5 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.

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 project elements that they are responsible, and for identifying and escalating any risks that are identified (via assessment or as a result of an incident) if it is outside their control to mitigate to an acceptable level.

6 Procedures for Maintaining Effective Information Governance

6.1 Meeting Legal Compliance

- The Company is registered for holding personal data as required under the Data Protection Act 1998
- 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
- 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 and therefore exempt from the Data Protection Act.
- Data subjects who data is recorded, or held in paper format by the Company are entitled, in law, to request details of information held about them and the Company must respond under arrangements in the Data Protection Act.

6.2 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,
- 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 the 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

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

6.3 Responding to data related incidents

In the event that 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 Act.[4]

6.4 Responding to subject access requests

Clinical Partners will respond to any written request for disclosure of personal data in accordance with the DPA.

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 fee (currently £10 for the supply of copies of electronic records and up to £50 for paper records)

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 see 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.

7. Process for maintaining confidentiality under the requirements of the Data Protection Act 1998

7.1 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.

[4] Details of how this is to be done and referral form can be found at: http://ico.org.uk/for_organisations/data_protection/lose

7.3 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.

8 Process for Monitoring Compliance with this policy

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

2. 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 spot checks/audits.

9. References and Related Policies and Procedures

- Clinical Partners Risk Management Strategy and Policy
- Data Protection Act 1998
- Information Commissioners web site http://ico.org.uk/