CONFIDENTIALITY

Name: NESI Professionals Ltd

Policy Statement

The policy outlined below adheres fully to the principles within Data Protection legislation the Freedom of Information Act 2000 and the Confidential Memorandum in place for local authority information purposes. All data held, stored or handled by this organisation complies with the current legislation and guidance.

This document outlines the policy of this organisation in relation to the handling of confidential information we need to hold about service users.

Definitions:

Confidential – means private, personal, intended to be kept secret

Private – belonging to or for the use of one particular person or group of people

It is important to make the above distinctions in order to fully understand our obligations in respect of confidentiality.

General

- The work of this organisation inevitably involves the need to know a good deal about our services users. We cannot provide good care without access to this information.
- Much of this information is highly personal and sensitive. We recognise that our service users have a right to privacy and dignity, and that this extends to our handling information about them in ways which cause as little as possible intrusion on those rights.
- We want our service users to feel at ease with the staff who help to care for them. An important element in that relationship is the capacity of a service user to be able to share information with staff, confident that it will be used with appropriate respect and only in relation to the care provided.
- As providing care is a complex process, it is not possible to guarantee to a service user that information they give about themselves will be handled only by the staff to whom it was first passed; however, we can ensure that information is seen only by staff on the basis of their need to know.
- We sometimes have to share information with colleagues in other agencies, but we only do so on the basis of their need to know and as far as possible only with the permission of the person concerned.
- We will only break the rule of confidentiality in very extreme circumstances which justify our taking that action for the greater good of a service user or, exceptionally, others.

Our Legal Obligations

Data Protection Legislation

Data Protection legislation lays various legal obligations on this organisation and similar organisations concerning the handling of the information we hold on individuals. Information must, for example, be obtained fairly and lawfully; be held for specified purposes; be adequate,

relevant and not excessive for the purpose for which it was gathered; be accurate and up to date; and not be held for longer than is necessary. We observe all of these requirements.

Please Note

Guidance on confidentiality and how it can be maintained in respect of service user information is now assisted by a wealth of information. Reference should be made to the following:

- Department of Health 2003 Confidentiality NHS Code of Practice
- National Institute for Health and Social Care Excellence
- Information Commissioner Codes of Practice
- Local Authority Confidentiality Agreements*
- Code of Practice on confidential information published by the Health and Social Care Information Centre December 2014
- Records Management Code of Practice for Health and Social Care 2016**

* These are usually found within the Local Authority Contract or Service Specification Documents issued to you as a provider of services. These will often have a set of procedures which are in addition to any other guidance.

** This Code of Practice is for providers working under contract to the NHS

The Caldicott Principles - Revised September 2013

Principle 1. Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Information and Care Needs Assessment

Every user of the services of this organisation must have their care needs thoroughly assessed before services are provided. This necessarily entails the staff who carry out an assessment, or handle assessment material sent to us from other agencies, learning a considerable amount about an individual. It is the duty of such staff to retain record and pass to the allocated care workers only the information that is relevant to the person's future care. A similar obligation applies to staff involved in a review or reassessment of care needs or in making any changes in the service provided.

Handling of Information by Care Workers

The care workers assisting a service user have access both to the information passed to them when they start to work with that service user and to knowledge which accumulates in the course of providing care. They have a duty of confidentiality:

- To treat all personal information with respect and in the best interests of the service user to whom it relates
- To share with their manager, when appropriate, information given to them in confidence
- To share confidential information, when appropriate, with colleagues with whom they are sharing the task of providing care
- To pass and receive confidential information to and from colleagues on occasions when they have to be replaced because of sickness, holidays or other reasons, in a responsible and respectful manner
- To pass confidential information to other social and healthcare agencies only with the agreement of the service user, with the permission of their manager, or in emergencies (when it is clear that it is in the interests of the service user or is urgently required for the protection of the service user or another person)
- To refer to confidential information in training or group supervision sessions with respect and caution and preferably in ways which conceal the identity of the service user to which it relates
- To never gossip about a service user or to pass information to any other individual other than for professional reasons.

Managerial and Administrative Responsibilities

Confidential information must occasionally be seen by staff other than the care workers providing direct care. It is therefore the responsibility of managers to ensure that information is stored and handled in ways that limit access to those who have a need to know, and to provide the following arrangements in particular:

- To provide lockable filing cabinets to hold service users' records and ensure that records are kept secure at all times
- To arrange for information held on computers to be accessed only by appropriate personnel
- To locate office machinery and provide appropriate shielding so that screens displaying personal data are hidden from general view.

Exceptional Breaches of Confidentiality

There are rare occasions in which it is necessary for a staff member acting in good faith to breach confidentiality in an emergency situation — for example, to protect the service user or another person from grave danger — without obtaining the permission of the person to whom it applies. In such circumstances, the staff member should use their best judgement, should consult the service user's representative—a manager or a colleague if possible—and should inform their manager of what has happened as soon afterwards as possible.

Related Policies

Co-operating with other Providers

Consent

Cyber Security

Data Protection Legislative Framework(GDPR)

Good Governance

Record Keeping

Services Users Records (HOME)

Training Statement

Staff Briefing, Training and Discipline

It is a responsibility of management to ensure that all relevant staff are briefed on this organisation policy and procedures on confidentiality, are trained in the implications of this issue, and have opportunities to explore any problems they encounter and be supported through appropriate supervision. Inappropriate breach of the rules of confidentiality will be treated as a disciplinary matter.