CONFIDENTIALITY POLICY

Scope

- **Policy Statement**
- Definitions
- General
- **The Policy**
- Our Legal Obligations
- UK Data Protection Legislation
- The Caldicott Principles – 2020
- Information and Care Needs Assessment
- Handling of Information by Care Workers
- Managerial and Administrative Responsibilities
- Exceptional Breaches of Confidentiality
- **Related Policies**
- **Related Guidance**
- **Training Statement**

Policy Statement

The policy outlined below adheres fully to the principles within UK data protection legislation, the Freedom of Information Act 2000 and the confidential memorandum in place for local authority (LA) 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 concerning the handling of the confidential information we need to hold about Service Users.

Definitions

Confidential: 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 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 of information about them in ways that 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 concerning the care provided.

- As providing care is a complex process, it is not possible to guarantee to a Service User that the 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 based on their need to know.
- We sometimes have to share information with colleagues in other agencies, but we only do so based on 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 that justify our taking that action for the greater good of a Service User or, exceptionally, of others.

The Policy

Our Legal Obligations

UK Data Protection Legislation

UK Data Protection legislation lays various legal obligations on this organisation and similar organisations concerning the handling of the information we hold on individuals. The 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.

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.
- LA confidentiality agreements. These are usually found within the LA contract or service specification documents issued to you as a provider of services. These will often have a set of procedures that are in addition to any other guidance.
- 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 for providers working under contract to the NHS

The Caldicott Principles - 2020

- **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**: **Do** not **use personal confidential data unless it is necessary.** Personal confidential data items should not be included unless it is essential for

the specified purpose(s) of that flow. The need for Service Users to be identified should be considered at each stage of satisfying the purpose(s).

- **Principle 3: Use the minimum necessary personal confidential data.** Where the use of personal confidential data is considered to be essential, the inclusion of each item of data should be considered and justified, so that the minimum amount of personal confidential data as is necessary is transferred or accessible 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.
- **Principle 8: Inform patients and Service Users about how their confidential information is used** A range of steps should be taken to ensure no surprises for patients and Service Users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required**.**

Information and Care Needs Assessment

Every Service User 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 who handle assessment material sent to us from other agencies learn 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 that 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, the 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 that 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.
- To anonymise Information that is shared for the benefit of the community. As a health and social care organisation, we clearly explain to Service Users and the public how the confidential information we collect could be used in de-identified form for research, audit, public health and other purposes.

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 need to know, and to provide the following arrangements in particular:

- Lockable filing cabinets to hold Service Users' records and ensure that records are kept secure at all times.
- For information held on computers to be accessed only by the 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, e.g. 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 (UK GDPR)

Good Governance

Record Keeping

Services Users Records (HOME)

Related Guidance

UK Data Protection Legislation:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Freedom of Information Act 2000:
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

Royal College of Nursing Confidentiality:
https://www.rcn.org.uk/

Codes of Practice for Handling Information in Health And Care:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care

A Data Protection Code of Practice for Surveillance Cameras and Personal Information:
https://ico.org.uk/media/about-the-ico/events-and-webinars/1043340/surveillance-by-consent-cctv-code-update-2015-jonathan-bamford-20150127.pdf

The Data Security and Protection Toolkit (DSPT)
https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/data-security-and-protection-toolkit/

Training Statement

All staff, during induction, are made aware of the organisation's policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary, and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used, including one to one, online, workbook, group meetings, and individual supervisions. External courses are sourced as required.

Date Reviewed: March 2024

Person responsible for updating this policy: Hitendra Sharma

Next Review Date: March 2025