

Data Protection and Confidentiality Policy

Reference: DSP DOC 01-1.2.1B

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 23/02/2021

Organisation Issue Date:

1. Purpose and scope

This policy:

- Sets out Organisation Name's commitment to the confidentiality of personal information and its responsibilities with regard to the disclosure of such information;
- << Content removed for sample purposes>>
- <<Content removed for sample purposes>>

2. Responsibilities

All employees, contractors and associates share the responsibility for ensuring that information assets are handled in accordance with this policy.

3. Definitions

Confidentiality: The ethical principle or legal right that a physician or other health and social care professional will hold secret all information relating to a patient/service user, unless they have given informed consent permitting disclosure.

Data: Information as defined by data protection law that is:

- Processed electronically i.e. information systems, databases, microfiche, audio and video systems (CCTV) and telephone logging systems;
- Recorded with the intention that it shall be processed by equipment; or
- Recorded as part of a relevant filing system, i.e. structured, either by reference to individuals or by reference to criteria relating to individuals which is readily accessible.

Data Controller: The individual, company or organisation who determines the purpose and the manner in which personal data may be processed.

Data Processor: Any person other than an employee of the data controller who processes data on behalf of the organisation.

Data Subject: A living individual who is the subject of the processed personal data.

Disclosure: The divulging or provision of access to data.

Personal Confidential Data: <<Content removed for sample purposes>>

Personal Information: <<Content removed for sample purposes>>

Processing: Using information in the following ways:

- <<Content removed for sample purposes>>

Special Category Personal Data (formally known as sensitive personal data): is any information about a person relating to their:

- <<Content removed for sample purposes>>

Third-party: Any person other than:

- <<Content removed for sample purposes>>

4. Data protection

The principles of data protection

Data Protection Law sets out the following principles to support good practice and fairness in processing personal information. These principles stipulate that:

- Personal data must be processed lawfully, fairly and transparently;
- Personal data can only be collected for specific, explicit and legitimate purposes;
- Personal data must be adequate, relevant and limited to what is necessary for processing;
- Personal data must be accurate and kept up to date with every effort to erase or rectify without delay;
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing;
- Personal data must be processed in a manner that ensures the appropriate security; and
- The controller must be able to demonstrate compliance with the other data protection principles (accountability).

Information security

In order to ensure the confidentiality of personal information, systems and

procedures are required to control access to such information. Such controls are essential to ensure that only authorised persons have:

- <<Content removed for sample purposes>>

Organisation Name's responsibilities for confidentiality and appropriate processing of personal data remain in place even if the processing is being undertaken by a third-party contractor.

Access to personal information

Individuals or persons, acting on the behalf of other individuals, with consent have a right of access to data held about them. This includes access to audit trails, that indicate who has accessed their personal or confidential data. The subject access procedure is set out in the [Subject Access Request Procedure](#).

5. Confidentiality

Duty of confidentiality

<<Content removed for sample purposes>>

The Caldicott Principles for protecting and using personal information

The Caldicott Committee's 1997 Report on the Review of Patient-Identifiable Information, found that compliance with confidentiality and security arrangements was patchy across the NHS and identified good-practice principles when handling patient information. This was revised in 2013. The principles are as follows:

1. <<Content removed for sample purposes>>

The role of the Caldicott Guardian

The Caldicott Committee report also led to the appointment of Caldicott Guardians.

Their role is to agree and monitor protocols for sharing information across organisational boundaries, ensure that patient's/service user's rights to confidentiality are respected, and safeguard the security of personal information.

<<Content removed for sample purposes>>

Disclosure of confidential information

The NHS has strict guidance on the disclosure of personal confidential data. Organisation Name complies with this guidance as part of its contractual

obligations.

Direct care purposes

<<Content removed for sample purposes>>

Non-care purposes

Individuals must give explicit consent for data sharing for the following non-care purposes:

- <<Content removed for sample purposes>>

More detail on non-care purposes is provided in Annex A of this policy.

Staff must be assured that there is a lawful basis before information is shared. Any queries on the legitimacy of sharing information should be directed to the Information Security Manager.

Any unlawful personal or confidential data sharing undertaken must be reported as an incident and investigated in line with the [Information Security Incident Management Procedure](#).

Objections to handling confidential data

<<Content removed for sample purposes>>

6. Data protection impact assessments (DPIAs)

New initiatives that involve high-risk processing of personal data will be subject to a DPIA to ensure the privacy and security of personal confidential data is maintained.

7. Information flow mapping

Flows of personal information into and out of Organisation Name will be mapped using the [Data Protection Impact Assessment \(DPIA\) Tool](#).

8. Overseas data transfers

<<Content removed for sample purposes>>

9. Implementation

<<Content removed for sample purposes>>

Document owner and approval

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).