Introduction

St Rocco's Hospice (the hospice) recognises the need to share information across organisational and professional boundaries in order to ensure effective co-ordination and integration of services for those who use our services.

The hospice also recognises the importance of security and confidentiality in relation to personal information and confidential information as contained in legislation, particularly the Data Protection Act 2018 (DPA18) and UK General Data Protection Regulation (UK GDPR) and data sharing codes of practice issued by the Information Commissioner's Office plus the common law duty of confidentiality.

The data sharing code of practice is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how DPA18 applies to the sharing of personal data.

It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one-off requests to share personal data.

Adopting the good practice recommendations in the code will help organisations to collect and share personal data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.

This policy covers two main types of information sharing:

'Systematic' which is routine information sharing where the same data sets are shared between the same organisations for an established purpose, e.g. reporting activity data. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes e.g. providing better patient care where information recorded in an electronic patient record system by whichever party is available to all subject to consent being obtained from the patient by each party

Ad hoc or 'one-off' information sharing where much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures, e.g. a subject access request. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation, e.g. Out of Hours access to a patient record, either by a community on-call doctor or Accident and Emergency department

This policy sets out the requirements placed on all hospice staff when sharing personal information with other partner organisations.

Compliance with Statutory Requirements

- Access to Health Records Act 1990
- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- UK General Data Protection Regulation
- Human Rights Act 1998

Related Policies / Procedures

- Anonymisation and Pseudonymisation
- Caldicott Plan
- Confidentiality
- Data Protection

- Data Quality
- Data Security and Protection Toolkit
- Forensic Readiness Policy
- ICO Anonymisation Code of Practice November 2012
- ICO Data Sharing Code of Practice December 2020
- Incident Reporting and Management
- Information Assets
- Information Governance
- Information Management
- Information Risk
- Information Security
- Local Registration Authority
- Mobile Working
- Network Security Policy
- Privacy Notices
- Subject Access Requests

Scope

The policy applies to all employees of the hospice and all staff working in or on behalf of the hospice including temporary staff (including locum doctors) contractors, secondees, volunteers, student doctors and nurses.

Information includes:

- Personally-identifiable data/information is anything which contains the means to identify a person, e.g. name, address, postcode, date of birth, and must not be stored on removable or mobile media unless it is encrypted
- Personal confidential data. Taken from the Caldicott Review, this term describes personal information about identified or identifiable individuals, which should be kept private or secret. Generally this is considered to be health related information, such as an NHS number. However it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc.
- 'Personal' includes the Data Protection Act 2018 (DPA18) definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the DPA18
- All records held in any format, whether paper-based or electronic format which includes laptops, removable media (USB sticks) mobile phones, cameras or even heard by word of mouth

Policy Statement

The hospice will enter into information sharing agreements with all partner organisations using mutually agreed Information Sharing Protocols, which will specify the mechanisms by which information can be shared and the content of the information flows, complying with all necessary legal requirements and codes of practice.

Similarly, the hospice will ensure that in all circumstances of information sharing, staff will:

- Comply with the law, guidance and best practice
- Provide only the minimum information necessary for the purpose of the sharing and shared only what the contract explicitly permits
- Respect individuals' rights, particularly confidentiality and security

- Adhere to confidentiality requirements unless there is a robust public interest or a legal justification for disclosure

The following factors will be taken into consideration when deciding whether to enter into an information sharing agreement, whether as provider, recipient or both:

- **What is the sharing meant to achieve?** There should be a clear objective or set of objectives. Being clear about this will identify the following:
- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data
- **What information needs to be shared?** All the personal data held about someone should not be provided if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies “Use the minimum necessary personal confidential data“
- **Who requires access to the shared personal data?** It is necessary to employ ‘need to know’ principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only have access to data if they need it to do their job and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties
- **When should data be shared?** It is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events
- **How should data be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security
- **How can we check the sharing is achieving its objectives?** Judgement is required to determine whether sharing is still appropriate and confirm that the safeguards still match the risks
- **How are individuals made aware of the information sharing?** Consideration must be what to tell the individuals concerned. Is their consent needed? Do they have an opportunity to object? How to take account of their objections? How to ensure the individual’s rights are respected and can be exercised e.g. how can they access the information held once shared?
- **What risk to the individual and/or the organisation does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals’ trust in the organisations that keep records about them?

It is good practice to document all decisions and reasoning related to the information sharing.

The data to be shared will be defined and agreed within an information sharing protocol. This will set out the necessary mechanisms to share relevant information appropriately. An overview of information sharing is provided in Appendix 2

Responsibility / Accountability

Chief Executive

The Chief Executive has overall responsibility for ensuring that information about individuals is shared appropriately and in accordance with all legal requirements.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) acts as the advocate for information risk on the Board of Trustees and internal discussions and provides written advice to the Chief Executive on the content relating to information sharing in the annual information risk report.

In addition to ensure that the hospice complies with DPA18 and that employees are fully informed of their own responsibilities for complying with the law.

Further to provide quarterly reports to the Information Governance Sub Group relating to information sharing.

Caldicott Guardian

The Caldicott Guardian is responsible for acting as “protector” of service user information.

The hospice Caldicott Guardian must approve all procedures that relate to the use of patient information and is responsible for the establishment of procedures governing access to and the use of patient-identifiable information and where appropriate, the transfer of that information across organisational boundaries. e.g. subject access requests.

Information Governance Lead

The Information Governance Lead is responsible for maintaining the currency of this policy and providing advice on request to any member of staff, in general, and the Chief Executive, SIRO and Caldicott Guardian in particular on the issues covered within it and giving advice and support on information handling standards and frameworks as required.

This includes:

- Confidentiality and Data Protection assurance
- Corporate Information Assurance
- Clinical Information Assurance
- Freedom of Information Assurance
- Information Governance Management
- Information Quality Assurance

Head of People and Culture

The Head of People and Culture is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

Heads of Department and Other Managers

Heads of Department and other managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon in line with the hospice incident reporting policy.

All staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Code of Confidentiality which the hospice operates. There is also a confidentiality clause in their contract of employment and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health or staff records or abuse of computer systems is a disciplinary offence which could result in dismissal or termination and must be reported.

Senior Leadership Group

The Senior Leadership Group (SLG) has strategic responsibility for the implementation and monitoring of this policy and to receive reports from the SIRO relating to information sharing.

Finance Sub Committees

The Finance Sub Committee is to be aware of and receive reports relating to the introduction and monitoring of information sharing from the SLG.

The Board of Trustees

The Board of Trustees is to be aware of and receive the annual report on the management of information sharing throughout the hospice via the Finance sub-committee.

Policy Monitoring and Review

This policy will be reviewed on a three yearly basis or more frequently if legislation or regulatory guidance or other hospice policies directly linked to this determine that the policy needs to be amended.

In addition, should an organisation which is a signatory to an information sharing protocol undergo an organisational change which could affect the continuing effectiveness of that protocol an extraordinary review can be requested at any time by either signatory.

Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

Audit plan

An annual review will be undertaken by the Chief Executive Officer, SIRO, Caldicott Guardian and IG Lead of all Information Sharing Protocols to ensure their continued relevance to hospice operations.

An annual, or more frequently if required, report will be prepared by the SIRO for the Finance sub-committee to inform the group and any other stakeholders, including trustees, of new or changes to existing protocols together with the actions taken to mitigate any additional risks identified.

Definitions

There are three broad categories of information relating to service users that the hospice may wish to collect, store and share and these are as follows:

Aggregated (Statistical) Information

Aggregated (Statistical) Information: Aggregate and management information used to plan and monitor progress of the hospice in its delivery of services and to manage its local focus so as to provide the most effective support to its service users and partner organisations.

This is generally outside of the remit of the Data Protection Act 2018.

Depersonalised/Anonymised Information

Depersonalised/Anonymous Information: Information that has had all person identifiable information removed (e.g. name, address, unique identifiers, etc.) so as to render it anonymous and is therefore outside the remit of DPA18.

Personally-identifiable Information
Personally-identifiable Information (including non-sensitive, confidential and sensitive data): Information (name, address, unique identifiers, etc.) relating to a living individual, including their image or voice, that enables them to be uniquely identified from that information on its own or from that and other information available to the hospice.

Confidential Information

There may also be 'Personally-identifiable Information', which is outside of that defined as 'special category' by DPA18 but which has been identified by the hospice as being of a personal and sensitive nature, known as "Professionally Sensitive Information" but more often called "Confidential Data".

Examples of this include patient or client characteristics e.g., substance misuse, opinions or assessment data.

Sharing Information

Information sharing can take the form of:
- A reciprocal exchange of data
- One or more organisations providing data to a third party or parties
- Several organisations pooling information and making it available to each other
- Several organisations pooling information and making it available to a third party or parties
- Exceptional, one-off disclosures of data in unexpected or emergency situations

In the context of this policy, information sharing means the disclosure of personal information by the hospice to a third party organisation or organisations.

Sharing Non-personal Information

Key information is shared with other organisations to:
- Improve patient experience
- Facilitate commissioning of services
- Manage and plan future services
- Facilitate quality improvement and clinical leadership
- Assure and improve the quality of care and treatment
- Statutory returns and requests
- Train staff
- Audit performance

Sharing Personal Information

Personal information may be shared with other organisations, where necessary and proportionate to:
- Investigate complaints or potential legal claims
- Protect children and adults at risk
- Assess need, service delivery and treatment

Data Sharing Code of Practice – December 2020
The ICO Data Sharing Code of practice can be found here:
https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf

Data Sharing Checklists for (1) Systematic and (2) One Off Requests

The ICO Data Sharing checklists can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/

Anonymisation Code of Practice – Nov 2012

The ICO Anonymisation Code of Practice can be found here
https://ico.org.uk/media/1061/anonymisation-code.pdf

Caldicott Principles

The eight Caldicott principles should be employed to examine the conditions under which patient-identifiable information is used or shared. The principles apply in all cases in relation to the management of patient identifiable information but in terms of this policy, principle 7 is of particular importance.

The Caldicott Principles can be found here:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf

Information Sharing Overview

Introduction

A high level agreement to share information should be reached and defined using an information sharing protocol, or a similar partnership agreement, particularly with partner organisations where information is shared on a regular basis.

The data to be shared should then be defined and agreed within an information sharing protocol. This will set out the necessary mechanisms to share relevant information appropriately.

Considerations

To ensure that the information can and will be shared, it is important to make sure that a number of questions are asked at this stage.

- Are all existing information sharing protocols and agreements available for review?
- Should the agreement relate to any associated information sharing protocols, partnership agreements and other strategic documents?
- Do partners understand why an agreement is needed and what its purpose will be?
- Are the context and scope of the agreement clearly defined and understood?
- Are the responsibilities of individual members of staff clearly defined and understood?
- Are the purposes for which information is required clearly defined and are the information requirements fully explored and understood?
- Has due consideration been given to the legality of sharing the information and its use once shared?
- Will the information be safe during transfer and after sharing?
- Have the appropriate communication channels been identified to ensure that the agreement and the consequences of sharing are known by the relevant people?
- Is there a process in place to feedback any problems in relation to access, the information, data quality etc.?

Changes to this policy

The hospice reserves the right to update or amend this policy at any time; please check on a periodic basis for the latest version