St Luke's
Hospice Plymouth

Confidentiality Code of Conduct



This document explains the St Luke's confidentiality code of conduct and how we will use it to deliver the best possible care.

Introduction

All employees working for a healthcare organisation are bound by a legal duty of confidence to protect the personal information that they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 2018 and, in addition, for healthcare and other professionals through their own professions' Code of Conduct.

The Confidentiality NHS Code of Practice further endorses this by providing a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. All employees of the organisation come into contact with confidential information at some level on a regular basis and as such need to be aware of their personal responsibilities to its use and protection.

Patients expect that information given to their doctors, nurses and other members of the health care team will be treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as employees.

Volunteers are also bound by a duty of confidence when volunteering within the organisation. The organisation must ensure that volunteers are not placed in a position or given a task that allows them access to data beyond that which they need to fulfil their role.

Legal Framework

St Luke's Hospice Plymouth is committed to compliance with all relevant UK and European Union legislation and NHS guidance. This includes but is not limited to:

- The NHS Confidentiality Code of Practice
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Caldicott Principles (see Appendix 1)
- Information Security Management: NHS Code of Practice
- Freedom of Information Act 2000
- The Copyright, Design and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- National Health Service Act 2006

Principles of Confidentiality

Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent. Confidential information may include personal information such as name, age, address and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.

Patients have a right to expect that a doctor, nurse or other members of the Health/ Social Care Team or the organisation's staff in general will not disclose any personal information learnt during the course of their duties, unless permission is given. Without assurance about confidentiality patients may be reluctant to give information that may be required in order to provide care.

Similar considerations apply to personal information concerning individuals, such as staff, donors and volunteers.

Confidential information may be known, or stored on any medium. Photographs, videos etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally. Information that identifies individuals personally must be assumed to be confidential, and should not be used unless absolutely necessary. Whenever possible, anonymised data (from which personal details have been removed and which therefore cannot identify the individual) is to be used instead. Note however that even anonymised information can only be used for justified purposes.

Awareness and Compliance

Everyone at St Luke's must be aware of the importance of confidentiality. All employees must be aware of their responsibilities for safeguarding patient confidentiality and keeping information secure. It must be remembered that no individual within the organisation has an automatic right of access to personal information held.

Employees must comply with requirements of the Confidentiality NHS Code of Practice, the Data Protection Act 2018 and the Freedom of Information Act 2000. Breaches of confidentiality are a serious matter and non-compliance may result in disciplinary action being taken.

Responsibilities

No employee shall knowingly misuse any information or allow others to do so. Any breaches/potential breaches of confidence are to be reported in accordance with the Incident/Near Misses Policy and procedure.

It is important that individual responsibilities towards the maintenance of confidentiality are known and understood:

- The Caldicott Guardian is responsible for overseeing and advising on issues of patient confidentiality.

- Managers are responsible for ensuring that all staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information within individual areas e.g. departments.

Individual employees are:

- Responsible for maintaining confidentiality. This duty of confidentiality is written into employees' contracts. Breach of confidentiality of information gained, either directly or indirectly in the course of duty will be considered a disciplinary offence that could result in dismissal.

- Authorised only to have access to personal information they need to know in order for them to perform their duties. Gaining access or attempting to gain access to information for any other purpose will be seen as a breach of confidentiality.

- Responsible for safeguarding the confidentiality of all personal and organisation information to which they have access, this includes its safe transfer and storage.

- Personally responsible for any decision to pass on information to another person/ third party.

- Responsible for adhering to the Confidentiality NHS Code of Conduct, Caldicott Principles, the Data Protection Act 2018 and the Freedom of Information Act 2000.

- Expected to treat any non-person identifiable information that could be considered sensitive to the business with the same degree of care as would be afforded to person identifiable information.

Guidance and support relating to the maintenance of confidentiality and security of information is available from the Caldicott Guardian and Clinical Director.

- The finance and fundraising databases contain confidential information relating to individuals, the Hospice and the Trading Company. Information held within these databases is to be accessed and shared according to individual's roles and should only be accessed and shared on a need to know basis in accordance with the Data Protection Act 2018 and the Freedom of Information Act 2000.

Acting on the Duty of Confidentiality.

Any personal information, non-clinical or clinical, must be treated as confidential. No personal information, given or received in confidence, may be passed to another person or organisation without the consent of the provider of the information. This is usually the patient but sometimes another person may be the source (e.g. relative or carer).

No personal information, given or received in confidence for one purpose may be used for a different purpose without consent of the provider of the information. This is the same with donors' information as with patient information.

Whilst patients usually understand and accept that information may be shared within the healthcare team in order to provide care, it is still necessary to check that the patient understands what will be disclosed and who may be contributing to their care.

It is also important to respect the wishes of any patients who object to their information being shared, except where this would put others at risk of death or serious harm.

The overriding principle is that patients, donors, staff or volunteers should not be shocked to find out how their information has or is being used or shared, rather that they should be effectively informed to allow them to exercise their rights in relation to their data.

The duty of confidentiality owed to a deceased patient is to be viewed as being consistent with the rights of living individuals. This also applies to the duty of confidentiality owed to a deceased donor whose details are held on the fundraising database.

Training and Awareness

Training and awareness of the importance of the maintenance of confidentiality and information security will be an on-going process throughout an individual's employment and will form part of the mandatory training programme.

Managers will be responsible for ensuring that employees are made aware of any specific departmental requirements/procedures.

Monitoring

The Caldicott Guardian and Clinical Director will provide regular reports to the Clinical Review Group:

- The number of reported 'information' untoward incidents including:
- Confidentiality
- Security
- Misuse of data
- Staff training undertaken

Appendix A

Caldicott Principles - Justify the purpose(s).

Question why information is required and what specific information is needed, to enable them to perform their task.

Don't use patient/client –identifiable information unless it is absolutely necessary.

Consider why identifiable information about a patient/client is being requested, whether it could be anonymised in some way, and if not what the benefits are, do they outweigh the patient/client's right to confidentiality.

Use the minimum necessary patient/client identifiable information.

Where supplying patient/client-identifiable information is vital, then we need to consider the absolute minimum required, for this we have to consider what is needed for and what they have a right to see.

Access to patient/client – identifiable information should be on a strict need –to-know basis.

Only those who need to view patient/client-identifiable data should be allowed access and even then only to that which they need to know.

Everyone with access to patient/client-identifiable information should be aware of his or her responsibilities.

Each member of staff concerned should be aware of the implications that a breach of confidentiality has on the patient/client or member of staff and what they should be doing to prevent or reduce the risk of any such breaches.

Understand and comply with the law.

All uses of patient /client –identifiable data should be lawful. Someone within your organisation must be responsible for ensuring that the organisation complies with legal requirements.

Further Contacts and Information
If you have any questions, then we would be happy to discuss this further with you. Our contact details are below:

Data Protection Officer | dpo@stlukes-hospice.org.uk
Information Commissioner's Office | www.ico.gov.uk
Care Quality Commission | www.cqc.org.uk

St Luke's Hospice Plymouth
Stamford Road
Turnchapel
Plymouth
PL9 9XA
Telephone: **01752 401172**

V4 | JJC
Review date: Feb 2027

If you need this leaflet in any other formats or languages, including braille, please contact us and we will provide as necessary.



St Luke's Hospice Plymouth is a charitable company limited by guarantee.
Registered in England No. 1505753. Registered Charity No. 280681