Policy: Information Governance

Purpose of this policy: to identify how the organisation will meet the key requirements of a wide range of information governance related matters; to set out and promote a culture of good practice in the processing of information and use of information systems that support the provision of high quality care of users and supporters of our services; to ensure that information is handled to ethical and quality standards in a secure and confidential manner.

Blythe House Hospice requires all employees and volunteers to comply with the policies, procedures and guidelines which are in place to support this policy.

Statement: Blythe House Hospice undertakes to ensure that information is managed appropriately with regard to confidentiality, the right to privacy of individuals and the requirements of the Data Protection Act 1998. The hospice will comply with all requirements of the Care Quality Commission and other statutory bodies requiring information to contribute to national health care studies and data sets.

Introduction

The availability of reliable information is an essential element in the delivery of appropriate and effective healthcare. It is used in

- effective management of individual patient care
- efficient management of services and resources
- monitoring of the organisation's performance
- day to day running of the hospice.

Information governance is a framework that enables the organisation to:

- establish good practice around the handling of information
- promote a culture of awareness and improvement
- comply with legislation and other mandatory standards.

Scope: this policy covers:

Systems: All information systems within the organisation, both electronic and paper based, fall within the scope of this policy. The organisation's information systems include patients, finance, risk, fundraising, volunteers, human resources and payroll databases.

Staff: All users of the organisation's information and systems including employees, volunteers and other individuals who have been authorised to access and use such information or systems.

Information: All information and data collected or accessed in relation to any Blythe House services, whether by employees or individuals and organisation under a contractual relationship with the hospice. All information stored on facilities owned or managed by the hospice or on behalf of the hospice belongs to the hospice unless proven otherwise.

Related Policies

The following policies are in place to support information governance:

- Confidentiality
- Records
- Hospice Governance
- Consent to Care & Treatment
- Volunteering
- Adverse Events
- Privacy and Dignity of Patients
- Care and Welfare of Service Users.
- Risk Management

Procedures and Guidelines

The organisation will achieve implementation of the policies through detailed procedures and guidelines for staff as appropriate and required.

Responsibilities

Trusted IT

- Ongoing server administration and risk assessment relating to Information Technology throughout the organisation

Hospice Director

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its stakeholders
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently
- Advising the trustees and management team on the information risk aspects of on internal controls.

Hospice Governance Group

The senior managers will take responsibility for the implementation of this policy.
All staff will receive the necessary guidance and information via the monthly staff meeting.

The Caldicott Guardian

The Hospice Director is the Caldicott Guardian with the following responsibilities:

- acting as a champion for data confidentiality at operational management level and as chairperson of the Hospice Governance group
- developing knowledge of confidentiality and data protection matters including links with external sources of advice and guidance
- ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- overseeing all arrangements, protocols and procedures where confidential healthcare information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

Incidents and Serious Incident Reporting

All incidents indicating a suspected or actual information security breach should be reported to your immediate line manager, an adverse event form completed and sent to the Hospice Director.

References

- Data Protection Act 1998, Norwich, T.S.O., The Stationery Office, 2003 (reprinted)
- The Caldicott Report 1997, Department of Health (DH) DH, London.
- The Public Records Act 1958
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- Code of Practice on Protecting the Confidentiality of Service User Information 2012
- Mental Capacity Act 2005
- Records Management: NHS Code of Practice 2009
- Current Performance Standards (NHS IG Toolkit) 2013
- Copyright, Designs and Patents Act 1988
- Companies Act, 2006, Office of Public Sector Information. Charity Commission News Issue 13 December 2000, Charity Commission, Liverpool
- Limitation Act 1980, Ministry of Justice
- Taxes Management Act 1970, H. M. Revenue & Customs