Confidentiality Policy 154

Introduction

Everyone working in the hospice is bound by a legal duty of confidentiality to protect the person-identifiable, sensitive or confidential information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also the requirements of the Data Protection Act 2018, UK GDPR and subsequent data protection legislation plus the common law duty of confidentiality.

It is important that the hospice protects and safeguards confidential personal and business information that it gathers, creates, processes and shares in order to comply with the law, relevant NHS regulatory requirements and to provide assurance to patients and the public.

This policy also sets out the requirements placed on all staff when sharing information within the hospice, plus externally with NHS and non-NHS organisations.

Information can be corporate as well as related to patients and staff (including temporary staff) however stored. Information may be held on paper, USB devices, computer files or printouts, laptops, mobile phones, digital cameras, in CCTV recordings or even heard by word of mouth.

Compliance with Statutory Requirements

- Data Protection Act 2018
- General Data Protection Regulation
- Access to Health Records Act 1990
- Caldicott Principles
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Human Rights Act 1998
- Information Security Management: NHS Code of Practice 2007
- NHS Confidentiality Code of Practice 2003
- Public Interest Disclosure Act 1998
- The Health and Safety at Work Act (1974)

Related Policies / Procedures

- Anonymisation and Pseudonymisation
- Caldicott Plan
- NHS Confidentiality Code of Conduct
- Data Protection
- Data Quality
- HSCIC Guide to Confidentiality 2013 (now managed by NHS Digital – but still the latest edition)
- Incident Reporting and Management
- Information Assets
- Information Management
- Information Governance
- Information Risk
- Information Security
- Information Sharing
- Photographs Permissions

- Protected Disclosure of Issues of Concern
- Removable Media
- Subject Access Requests

Scope

This policy applies to all persons (including hospice employees, volunteers, students, researchers, service providers, visitors, contractors or any other persons who have access to confidential hospice or service user information of any kind, no matter how obtained whether on hospice premises or in other locations.

All persons working within the hospice, receiving care from the hospice, their relatives or friends, and supporters are entitled to know that their personal information will be managed confidentially. Also, that such information will only be used for the purposes for which consent was given or for which a lawful basis for processing has been determined by the hospice.

All persons who contribute to the hospice can similarly be assured that their personal information will be managed confidentially and only used for the purposes for which consent was given, e.g. donors who Gift-Aid their contributions. This policy applies to all personal information, however processed, stored on computer or relevant filing systems (e.g. manual records) or Close Circuit Television and any extracts taken either printed, copied, or verbal.

Confidential information within the hospice is commonly thought of as health information. 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. It also includes hospice confidential business information.

Policy Statement

The lawful and correct treatment of personal information is vital to the successful operation of and maintaining confidence within the hospice and the individuals with whom it deals.

Therefore, the hospice will, through appropriate management, apply the following rules for confidentiality:

1. Confidential information about service users or patients should be treated confidentially and respectfully by:

    - Maintaining trust and respect as a priority
    - Respecting professional confidentiality obligations
    - Ensuring the care record is as complete as possible, accurate and fit for purpose

2. Members of a care team should share confidential information when:

    - It is needed or the safe and effective care of an individual
    - It is relevant, necessary and proportionate
    - There is an absolute imperative because of a threat to the safety of others e.g. safeguarding

3. Data that are collected while providing direct care can provide benefits for the community. Where lawful justification exists, anonymised data may be used for a purpose other than direct care, e.g. to support the improvement of care services.

    - In exceptional circumstances it may be necessary to share confidential information, but this requires informed consent or that there is a legal obligation to share for a particular purpose e.g. in the public interest
    - Confidential information can be shared when there are sufficient controls to ensure a 'trusted environment' e.g. an information sharing agreement with restrictions on linking information to prevent the re-identification of individuals or, where a secure data processing agreement in in place between all parties concerned with the processing.
    - For all the lawful methods of sharing information, the following three conditions should be met:
    - Individuals should be informed about how their confidential information may be shared or used, with whom and why
    - The minimum amount of confidential information should be used to support the purpose for which it is collected
    - Data protection legislation should be checked to ensure there are no legal restrictions on sharing particular pieces of information

4. An individual's right to object to the sharing of their confidential information should be respected, the considerations being:

    - Objections should be considered consistently and individuals should receive a n explanation of the likely consequences of their actions
    - When individuals object to the sharing of confidential information by the hospice, confidential information will not be shared
    - When an objection to the sharing of confidential information, anonymised information can be shared which will respect their wishes
    - Where the likely consequences of an objection pose such a significant risk that the objection is lawfully overruled, individual should receive an explanation e.g. in relation to a notifiable disease

5. The hospice should put policies and procedures in place to ensure the rules for confidentiality are followed, which will include:

    - Appointing a senior individual responsible for ensuring the confidentiality rules are followed
    - Completing an annual Data Security and Protection Toolkit Assessment
    - Ensuring that all organisations with which it shares information are committed to following confidentiality rules
    - Encouraging people to report concerns that the confidentiality rules have not been followed

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per the hospice Removable Media Policy or a business case has been approved by a member, or members of the Information Governance Sub Group.

In addition it is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other

persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the hospice. If staff have concerns about this issue, they should discuss it with their Line Manager or Information Governance Lead or SIRO

Any breach of confidentiality, inappropriate use of health records, staff records or business sensitive/confidential information, or abuse of computer systems could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

A summary of Confidentiality Do's and Don'ts can be found in Appendix A.

Responsibility / Accountability

6.1 Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that the hospice policies comply with all legal, statutory and good practice guidance requirements.

6.2 Senior Information Risk Owner

The Senior Information Risk Owner is responsible for ensuring the implementation of the requirements outlined within this policy and ensuring that training is provided for all staff groups to further their understanding of the principles and their application and that confidentiality is included in corporate inductions for all staff.

6.3 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of Caldicott Principles with respect to patient-identifiable information.

6.4 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 on the issues covered within it. In addition, to investigate reported incidents and escalate serious breaches to senior information governance management if required.

6.5 Head of People and Culture

The Head of People and Culture is responsible for ensuring that the contracts of all staff are compliant with the requirements of the policy.

6.6 Line Managers

Line 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 in line with the hospice incident reporting process. Managers are also expected to support staff with the completion of an incident reporting form if required.

6.7 All persons who come into contact with confidential information

Confidentiality is an obligation for all staff and those working on hospice premises. There is a confidentiality clause in their contract and that they are expected to participate in induction, training and awareness-raising sessions carried out to inform and update staff on confidentiality issues.

All persons should report confidentiality breaches using the hospice Information Governance incident reporting form and check with their line manager to assist with its completion if necessary.

6.8 Information Governance Subgroup (IGSG)

The IGSG oversees the development and implementation of Information Governance in the hospice and ensures that the organisation complies with supporting the legal and where appropriate the NHS regulatory framework with regard to information governance.

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.

Staff training requirements

Confidentiality training will be undertaken as outlined below. Should addition training be required this will be in agreement with the individual staff member and their immediate line manager.

User Group	Training Method: Email Cascade (Awareness) eLearning/Workbook Practical Assessment Group Training Session	Facilitator	Target Completion Date
New Staff	All new staff members will be provided with confidentiality training by the Information Governance Lead as part of their induction process to provide a hospice specific context to the general confidentiality training with in their eLearning	IG Lead	As part of their induction
New Staff	In addition general eLearning training will be undertaken as part of their induction	HR	As part of their induction
All Staff	eLearning	HR	Annually
All Staff	An Email cascade will be used to inform staff of revised policies	IG Lead	Within 10 days of policy ratification

Audit plan

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems and also procedures to evaluate the effectiveness of controls within these systems.

This hospice will establish appropriate confidentiality audit procedures to monitor access to confidential person-identifiable information.

Audits will be carried out no less frequently than annually – see Appendix 3 for audit plan

This function will be co-ordinated by the Information Governance Sub Group in conjunction with the electronic patient record System Administrators and Information Asset Owners and Administrators.

Definitions

As defined within this document

Appendix 1 – Confidentiality Do's and Don'ts

Do

- Safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working for or on behalf of the hospice
- Clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised
- Switch off computers with access to person-identifiable or business confidential information, or lock them if you leave your desk for any length of time
- Ensure that you cannot be overheard when discussing confidential matters so that confidential information is not disclosed accidentally
- Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know
- Share only the minimum information necessary
- Transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account. If this is not feasible, password protect files and send password separately
- Seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken
- Report any actual or suspected breaches of confidentiality
- Participate in induction, training and awareness raising sessions on confidentiality issues
- Minimise the amount of person-identifiable information taken away from the hospice e.g. on home visits. Any such information taken away from the hospice must be kept securely and confidentially
- Shred person-identifiable and confidential information in paper format when no longer required

Don't

- Share passwords or leave them lying around for others to see. You must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal
- Share information without the consent of the person to which the information relates, unless there are statutory grounds to do so
- Use person-identifiable information unless absolutely necessary and if necessary, anonymise the information where possible
- Collect, hold or process more information than you need and do not keep it for longer than necessary
- Forward any person-identifiable or confidential information via email to your personal e-mail account
- Store person-identifiable or confidential information on a privately owned computer or device

Appendix 2 – HSCIC Guide to Confidentiality 2013

The complete version of the Guide to Confidentiality in Health and Social Care document 2013 can be found on this NHS Digital website link:

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-guide-to-confidentiality-in-health-and-social-care/a-guide-to-confidentiality

Appendix 3 – Confidentiality Audit Plan

Department(s)……Date(s):……

#	Check	Findings			Recommended Improvements	Responsible	Deadline
		Y/N	Risk Rating	Comments			
Physical Security							
1	ID Badge pass being worn?						
2	Doors, Windows and locking systems operational?						
3	Visitors supervised?						
4	Restricted access areas secure?						
5	Filing cabinets/rooms kept locked?						
Computing Systems							
6	Password access required for all systems?						
7	Are passwords known by others?						
8	Computer screens kept locked when away from desk?						
9	Can sensitive information on screen be seen by members of the public / non-authorised staff?						
10	Access to folders restricted?						
11	USB ports disabled?						

12	Are all laptops encrypted?						
13	Is any personal / sensitive data kept on the laptop desktop?						
14	Email - how is personal / sensitive data emailed?						
15	Smartcards are not left in computer when away from desk?						
Filing							
16	Are cabinets lockable?						
17	Where are cabinet/desk drawer keys stored?						
18	Who has access to filing cabinets?						
19	Are clear desk processes followed?						
20	Are any personal /sensitive data left out in office?						
Staff Awareness							
21	Undertaken IG Mandatory training?						
22	Know where staff guidance is?						
23	Know who is IG Lead?						
24	Know who SIRO is?						

25	Know who Caldicott Guardian is?						
26	Know how to report an IG incident?						
Confidential Waste Processes							
27	Know who to contact to dispose of confidential waste securely?						
28	Any other observations						
Signed by: (Team Carrying Out the Audit) Date:							