Cornwall Hospice Care
Caring for our community
Mount Edgcumbe Hospice St. Julia's Hospice
Registered Charity No. 1113140

Organisational Information and Records Policy

Title:	Organisational Information and Records Policy
Procedural document Type:	Policy
Reference:	CL - 036 V1
Version:	Version 1.0
Approved by:	Clinical Governance
Date Approved:	13.3.19
Ratified by:	Clinical Governance
Date Ratified:	13.3.19
Name or originator/author:	Richard Ward
Name of responsible team:	Information Governance
Review Frequency:	3 years or when changes in legislation occur
Review Date:	February 2022
Target Audience:	Information Asset Owners and all staff and volunteers

Contents

Policy Statement

Information is one of the most valuable assets that Cornwall Hospice Care (CHC) holds. A hospice depends on the commitment and ability of its staff to deliver high quality care, to raise funds and manage its affairs. To achieve this, reliable information must be available when needed in appropriate forms.

This policy sets out the principles by which information is to be managed within CHC.

Review and amendment Log

Version No.	Type of Change	Date	Description of Change
Version 1	New	Feb 2019	New document

Introduction

1. Information is one of the most valuable assets that Cornwall Hospice Care (CHC) holds. A hospice depends on the commitment and ability of its staff to deliver high quality care, to raise funds and manage its affairs. To achieve this, reliable information must be available when needed in appropriate forms.
2. This policy sets out the principles by which information is to be managed within CHC.

Patient Information

3. Patient information is dealt with as a special case in the Health Records Policy.

General Information

4. It is recognised that information:
    a. may be held on paper, in electronic media, or in the memories of individuals;
    b. has value to CHC and other organisations when it is used effectively;
    c. is a fundamental component of evidence-based practice;
    d. carries costs in terms of its production, storage, retrieval, communication and disposal, which should be controlled by good information management.
    e. can be sensitive and require effective protection as required by good practice, contractual and moral obligations and the law;
5. Information generated or received in the performance of CHC services is the property of CHC.
6. It is the responsibility of all staff and volunteers who have access to information relating to CHC to take appropriate care of it and manage it in compliance with the requirements set out here. Failure to do so could result in disciplinary action.
7. CHC recognises the requirement for mutual assurance in respect of Information Governance arrangements when working with other services. e.g. CHC will work towards:
    a. compliance with established standards as permitted by the resources available such as the NHS Data Security and Protection Toolkit;
    b. joint working with partner organisations to establish secure, effective communications and integrated information governance arrangements;
    c. anticipating and meeting the reasonable requirements of commissioning and funding organisations.

8. CHC will have in place policies and/or procedures for:
    a. providing information for data subjects, patients and other service users;
    b. liaison with the press and broadcasting media;
    c. responding to requests for information from the public;
    d. ensuring compliance with:
        i. General Data Protection Regulations
        ii. Data protection Act 2018
        iii. Human Rights Act,
        iv. Common Law confidentiality,
        v. Health & Social Care Act,
        vi. Crime and Disorder Act,
        vii. Protection of Children Act.

    } in respect of sharing information with other agencies

Definitions

9. The Data Controller is a role set out under the GDPR. CHC is a 'Data Controller'. The Data Protection Officer is the designated person responsible for registration with the Information Commissioner's Office.

10. Confidential Information is defined as information that has commercial or other value to the CHC or others; it should be securely stored and communicated only to those who are authorised to receive it.

11. Personal Information is information by which a person may be identified either directly, or indirectly in combination with other information.

12. Personal Sensitive Information It is confidential and includes information relating to any of the following:

    a. racial or ethnic origin;

    b. political opinions;

    c. religious beliefs or other beliefs of a similar nature;

    d. membership of a trade union;

    e. physical or mental health condition;

    f. sexual life;

    g. the commission or alleged commission of any offences or any

proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any Court in such proceedings.

Duties

13. General responsibilities in respect of this policy are set out in the Governance Policy.

14. In respect of this policy, the following additional accountabilities and authorities are established.

15. The Finance Director is the Senior Information Risk Owner.

16. The Finance Director is the designated Data Protection Officer (as defined by the GDPR).

17. The Medical Director is the designated Caldicott Guardian for the organisation.

18. CHC is committed to establishing the necessary understanding and personal discipline needed to ensure that good information practices are maintained. This is primarily the responsibility of Information Asset Owners – supported by the Information Governance Officer and the staff of the IT Department.

19. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

General Principles

20. This Policy supports compliance with the General Data Protection Regulations and the Data Protection Act 2018 and should be read in conjunction with the CHC Data Protection Policy.

21. The confidentiality requirements of the CHC 'Code of Conduct' in the staff handbook and within the Data Protection and Confidentiality Section of the Volunteer Handbook must be met at all times. The principles set out here complement and support that Code and Volunteers Handbook.

22. The approach to be taken to information governance will be informed by systematic assessment of risk.

23. All staff and volunteers are required to maintain their awareness of current systems and practice used in their area of work.

24. The transmission of information can be done using paper, electronically or by word of mouth; when communicating sensitive information, appropriate methods must be used to ensure that the information is communicated and available only to those who are intended and authorised to receive it.

25. Information is not the property of any one individual. A balance must be struck between the essential protection of information and the need to make it readily available to those who need it for the performance of their work.

26. All planned major organisational change should include a data privacy impact assessment.

27. Information held must be:

    a. processed fairly and lawfully;

    b. relevant and adequate for purpose - complete and not misleading;

    c. accurate and up to date;

    d. necessary for the performance of identified tasks;

    e. secure against unauthorised or unlawful processing and accidental loss, destruction or damage;

    f. processed in accordance with the rights of the data subjects where these apply;

    g. not held beyond the time when it is required for the identified tasks, or for other, permissible reasons (such as approved research or compliance with legal obligations);

    h. destroyed when no longer used for the identified tasks.

28. A lawful basis for processing data must be data must have been identified for all personal data. This may be any one of the following:

    - consent,
    - processing is necessary for performance of a contract,
    - necessary for compliance with a legal obligation,
    - necessary to protect the vital interests of the data subject,
    - necessary for the performance of a task in the public interest or,
    - legitimate interest

29. Privacy notices will be provided to all data subjects. These will include information relating to who we are, what information is being collected, who is collecting it, how is it collected, why is it being collected, how will it be used and who will it be shared with?

30. Implicit in these rules is a requirement to ensure that, where information is shared with partner organisations, those organisations have adequate provisions in place for data security and are bound by confidentiality.

31. Guidance on the Archiving and Destruction of Records is contained in Appendix A.

Subject Access Requests

Access to Personal Information CHC Hold

32. Under GDPR all staff, volunteers, patients, customers, donors (literally anyone that CHC hold personal data about) have the right to see and receive a copy of that information. This is known as the data subjects 'right of subject access'.

Who can apply for access to personal information

33. Under the GDPR/Data Protection Act 2018 you can apply for access if you are:

- The data subject (you may apply for access to your own records)
- The data subjects representative. This could be a person with parental responsibility for a child (unless the child is 8-14 and is capable of understanding and consenting, then their consent is needed),
- a person authorised in writing by the data subject to act on their behalf,
- or a person appointed by the court to act on behalf of the data subject.

Can information be withheld?

34. The data subject, or the data subject's representative, has the right of access to information contained within the their record, except where:

- Any information that identifies a third party, where the third party is not a health professional and has not consented to the disclosure
- Any information which is restricted by law from disclosure under other Acts of Parliament.

How to apply

35. To formally make an application, you must do so in writing- please see the 'CHC Subject Access Request Policy and Procedure' which can be found on the CHC website or requested from the HR department which contains the full procedure and application forms. Once a completed application form has been received and considered, you can expect to receive a copy of your records within 1 month.

What to do when an error occurs

36. If there is a breach of confidentiality or records are lost/stolen the process described in Appendix B should be followed and an incident form must be completed (Appendix C). Any incidents relating to data protection /confidentiality issues must be notified to the line manager, service lead and Director of Finance (DPO) on the same working day. Each situation will be assessed on a case by case basis with the support of the manager.

37. The aim of reporting incidents is to make timely improvements to information quality by providing a record of issues that can be addressed rather than wait for a record keeping audit.

38. If a breach is found to be serious this may result in the disciplinary procedure being implemented which could result in dismissal.

39. If a breach is considered to be serious it must be reported to the Information Commissioner's Office within 72 hours of the organisation becoming aware of the breach. The risk will be assessed, and the report made by the Data Protection Officer. Failure to do this may result in a fine up to 20million euros or 4% of the organisation's turnover (whichever is higher).

40. When a breach is likely to result in a high risk to the rights and freedoms of the individual, they must be informed of this breach.

Monitoring and Review

36. This policy will be reviewed every three years by the Information Governance Forum.

37. Information 'incidents' (e.g. breaches of confidentiality or significant loss or risk to information) will be reported to the Finance Director (DPO) and reports considered by the Executive Management Team and the Information Governance Forum on a quarterly basis.

Training, Education & Development Required

38. Information Governance training will be provided to all staff and volunteers at induction and annually (for those hospice based) and every two years for other staff.

39. All staff using computers will be provided with instruction on CHC procedures for the effective creation, storage and retrieval of information. This will be done as part of induction.

References and Relevant Legislation

Human Rights Act 1998
Common law of Confidentiality (Case Law)
General Data Protection Regulations
NHS Data Security and Protection Toolkit
Data Protection Act 2018
Freedom of Information Act

Appendix A - Guidance on the Archiving and Destruction of Records

Archiving Documents

When records are no longer in use for current business purposes they should normally be destroyed unless they are listed for retention for legal or other reasons.

It is strongly recommended that each line manager considers the (legal) requirement for timely destruction of records at the point the records are created. Good practice in administration makes it easier to identify those records which are due for archive or destruction.

'The Cornwall Hospice Care Records Retention Schedule' gives the retention periods for records held by the CHC. These may not be fully comprehensive and it is emphasised that, if there is any doubt as to whether a record should be archived or destroyed, the appropriate line manager must be consulted.

Significant costs and risks are associated with the maintenance, storage and destruction of records, in both paper and electronic forms. It is therefore important that the Policies and guidelines on information (records) management are implemented reliably.

Each department must review its records at least annually to identify:

- those which are no longer in use and are due for archiving, and
- those which should be destroyed (including those documents previously archived).

Confidential waste bins are strategically based throughout the Charity and these are regularly, or on request, emptied by a 3rd party under contract. These are for the disposal of shredded or non-shredded confidential papers.
Archived records should be batched according to:

- the date at which they are scheduled for destruction;
- the type of record (e.g. pensions data, clinical records etc);
- the Department responsible.

Batches should be placed in secure boxes, separated for ease of identification and selection for destruction in due time.

Mixing of records due for disposal at different dates, or for disposal by different methods, in the same box must be avoided. Mixing of records imposes the need for a second selection process for destruction and increased costs.

Retention of Records Prior to Destruction

Please see the Cornwall Hospice Care Records Retention Schedule for the retention period for paper and electronic records. This schedule will be updated when new records or the retention periods of existing records are added or changed. Please see the up to date version of this schedule in the Policies and Procedures section of the CHC Intranet.

Destruction of records

It is the responsibility of each department to review its archived records on an annual basis to identify which items are to be destroyed.

Records are to be destroyed when they are no longer legitimately needed for the performance of the activity they were collected for or once they have been retained beyond the statutory retention period.

Records must be destroyed in such a way as to ensure that confidentiality is not breached. This will usually be by shredding the entire content of the record if held on paper or card, cross shredding if a medical record, or by securely deleting the content of records held on electronic media.

Where a large or substantial number of confidential records need to be destroyed the Maintenance Team should be contacted and they will arrange for the records to be collected and securely destroyed. A certificate of destruction will be provided by the company carrying out the destruction of confidential waste.

A record of what has been destroyed must be kept by the individual department.

Appendix B – Information Incident Reporting

In the event of a suspected information security or confidentiality breach occurring the following process should be followed:

All incidents, suspected incidents and near misses should be reported as soon as practically possible (normally within 24 hrs)

- The person discovering an actual or suspected information breach or incident should report it to their line manager (this includes near misses), and
- The line manager should ensure action is taken to contain the incident/prevent a recurrence.
- The incident should be reported to the area's Executive management, and
- an Information Incident Report form should be completed and sent to the Information Governance (IG) Officer (rward@cornwallhospice.c.uk).
- IG will carry out an assessment and determine, in conjunction with management, what investigation is needed,
- who should carry it out and
- who should receive the report.
- The IG Officer will ensure the Caldicott Guardian is made aware of the incident.
- All reported IG incidents are logged onto the NHS Incident Reporting system, and
- reported through the IG Forum.

The Information Incident reporting form is located in the Information Governance/Public IG Library folder on the CHC Intranet (Office 365), or may be obtained by contacting the IG Officer by email or on 01726 66868 Option 7.

Appendix C – Information Incident Reporting Form

INFORMATION INCIDENT REPORTING FORM

Location of incident:

Date of incident:

Which of the following best describes the incident *(please tick one):*

Lost digital equipment eg laptop computer	
Theft of digital equipment eg laptop computer	
Lost information (paper/digital eg USB stick)	
Theft of information (paper/digital eg USB stick)	
Information Breach - Post	
Information Breach - EMail	
Information Breach - Fax	
Other Breach of Information Security	

Other (please specify):

Details of the incident (please focus on facts rather than opinions):

Immediate action taken (if any):

Further planned/required actions (if any):

Form completed by: _____ Date:

Please return to: **Richard Ward** (information Governance Officer)

rward@cornwallhospice.co.uk

Tel: 01726 66868 Option 7