Thames hospice

Policy: CONFIDENTIALITY POLICY

Date	Author	Approved by	Doc name	Comment	Responsible Committee	Next Review
June 2019	Head of Governance and Quality & SIRO	Governance Committee	IG-P-0002	June 2019 Policy reviewed. Change to SIRO noted. Minor other updates. Appendices revised. January 2018 Policy reviewed in light of GDPR. Appendices revised and renewed. June 2017 Policy reviewed. Minor changes to text and layout. July 2015: Policy reviewed and updated. Policy Created: January 2004	Governance and Health and Safety Committee	June 2021

Policy Summary

This policy aims to support staff in making decisions on the management of confidential information. It does not seek to provide for all eventualities but to raise awareness of where or from whom to seek further guidance. It covers all Thames Hospice staff whether clinical or non-clinical.

1. The Data Protection Officer is the Head of Governance and Quality.
2. The Caldicott Guardian is the Director of Patient & Family Services.
3. The Senior Information Risk Owner (SIRO) is the Thames Hospice CEO.

1 Purpose of Policy

1.1 Patients, family members and supporters are assured that information given by them will only be used for the identified purposes(s) for which it was shared. Staff receiving, recording and sharing information are aware of their professional and organisational accountabilities with relation to maintaining confidentiality of information, and staff will always seek and record relevant consent with regard to obtaining an individual's information, clearly explaining the reasons why.

1.2 Thames Hospice will ensure confidential data is kept securely, shared only where appropriate and destroyed in line with current legislation.

1.3 The Hospice will process and use all information in accordance with current legislation, including but not limited to the current Data Protection Act (2018), and Caldicott Guidelines.

1.4 This policy aims to support staff in making decisions on the management of confidential information. It does not seek to provide for all eventualities but to raise awareness of where and from whom to seek further guidance (Data Protection Officer / Caldicott Guardian / SIRO).

2 Responsibilities

2.1 Ultimate Responsibility - Chief Executive Officer

2.2 First Line Responsibility.

2.2.1 Data Protection Officer (Head of Governance and Quality).

2.2.2 Caldicott Guardian (Director of Patient and Family Services).

2.2.3 SIRO (Head of Information Governance and Quality).

2.2.4 Data Asset Owners (Senior Managers in whose department data is held/used).

2.3 Operational Responsibility

2.3.1 Chief Executive Officer - Overall responsibility to ensure that the policy is fit for purpose and disseminated throughout the organisation.

2.3.2 Senior Management Team and Line Managers: ensuring their staff are implementing policy and guidelines in everyday practice.

2.3.3 All staff and volunteers.

2.3.4 Visiting professionals must maintain confidentiality regarding their access to privileged information.

2.3.5 Contractors must maintain confidentiality regarding their access to privileged

information in the course of their work and will be expected to sign confidentiality agreements.

3 Policy Statement

3.1 This policy applies to all members of staff and volunteers and those persons who may work in the hospice on work experience or secondment, or as a contracted service provider.

3.2 All persons working within the Hospice, receiving care from the Hospice, their relatives or friends, and supporters are entitled to be treated knowing that their personal information will be managed confidentially and only used for the purposes for which consent was given.

3.3 Guidance for patients and service users is given in the 'Confidentiality and Your Records' leaflet.

3.4 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. (*An example being donors who Gift Aid their contributions.)

4 Policy Detail

4.1 <u>What is confidential information?</u>

4.1.1 When one person discloses personal information to another, e.g., patient to doctor/nurse, or a Thames Hospice donor giving the Hospice information for Gift Aid recording purposes, in circumstances where it is reasonable to expect the information will be held in confidence, a 'duty of confidence' arises.

4.1.2 Information that can identify individuals must not be used or disclosed for purposes other than for which it was given without the individual's explicit consent.

4.1.3 Confidential Healthcare information: In gathering information to support its healthcare provision Thames Hospice is entrusted by, and expected by the individual to respect their privacy and act appropriately. Even if a patient may lack competence to extend this trust, (for example they might be unconscious), this does not diminish the expectation of the duty of confidence. A key guiding principle is that a patient's health record is made by the service to support their healthcare.

4.2 Who to approach for assistance and advice on disclosure issues?

4.2.1 No confidential information can be disclosed without consulting the Thames Hospice Head of Governance and Quality, who is the Hospice's Data Protection Officer.

4.3 Obligations of staff

4.3.1 All staff are expected to put the principles of this document and reference documents into practice at all times. If they are unsure, they must always seek advice from the Head of Governance and Quality.

4.3.2 Use of Memory Sticks or other removable recording devices. - Staff must never put personal identifiable data onto an unencrypted memory stick or other removable recording device.

4.4 Reporting Incidents

4.4.1 Any observed or overheard breach of confidentiality must be reported following the Thames Hospice Incident Reporting Policy (CG-P-0006).

4.4.2 Breaches in confidentiality will be treated extremely seriously. There is the potential for both the individual and the organisation to be prosecuted for serious breaches of the Data Protection Act.

4.4.3 Any breach of confidentiality may be dealt with using the Thames Hospice Disciplinary Procedures. Sanctions will be commensurate with the risk assessment and investigation findings but could ultimately lead to dismissal.

4.4.4 All incidents will be reported at the Governance and Health and Safety Committee and to Committees of the Board as appropriate.

4.5 Staff Training Requirements

4.5.1 Staff: All staff will be issued with a copy of the Staff Handbook on commencing work and will be required to read it and sign to say they have read this policy document and code of conduct.

4.5.2 Volunteers: All volunteers will be issued with a copy of the Volunteer Handbook on commencing work and an Information Governance leaflet.

4.5.3 Line Managers will reinforce specific confidentiality issues related to the individual's job role as part of their induction training, drawing their attention to specific processes within their work areas.

4.5.4 Staff are required to undertake annual Information Governance Training as part of the Mandatory Training Programme.

4.5.5 Staff are made aware of the Accident and Incident Reporting Policy and procedure; and, as part of their induction process with their Line Manager, they know how to contact the Data Protection Officer, and the Caldicott Guardian.

4.6 Audit Plan

4.6.1 Any formally identified breeches of confidentiality will be investigated on an individual basis.

4.6.2 Topics relevant to the implementation of this policy are included on the annual audit programme.

5 Breach of Policy

5.1 Any deviation in practice from the above policy and procedure will be deemed a breach of policy.

5.2 Any breach of this policy by Thames Hospice employees may lead to formal disciplinary action.

5.3 Any breach of this policy by Thames Hospice volunteers may lead to formal action under the Problem Solving Policy and Procedure.

APPENDIX 1 - <u>Definitions</u>

Patient or Person Identifiable Information includes:

- Name, address, full postcode, date of birth.
- Pictures, photographs, videos, audio-tapes and other images of patients.
- NHS number and local patient identifiable codes.
- Codes allocated to individual on databases.
- Anything else that may be used to identify an individual directly or indirectly, for example, a rare diagnosis, drug treatments, or statistical analyses which have very small numbers within a small population that may enable identification.

Anonymised Information: this is information which does not directly, and which cannot reasonably be used to, determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. Anonymised information is not confidential and may be used with fewer constraints.

Pseudonymised Information: as above but may have an attached code so that it can still be identified by those who have the code or index, maintaining a link with the original data.

Explicit or express consent: Consent clearly articulated by the patient or individual – may be verbal or written.

Implied consent: agreement signalled by behaviour.

Disclosure: divulging or provision of access to data.

Healthcare purposes: all activities that directly contribute to the diagnosis, care and treatments of an individual and the audit/assurance of the quality of the healthcare provided. Healthcare purposes do not include research, teaching, financial audit and other management activities.

Medical Purposes: as defined in the Data Protection Act include but are wider than healthcare purposes and include preventative medicine, medical research, financial audit, and management of healthcare services (including social care).

Information sharing: the documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality and data destruction between two or more organisations.

Public interest: exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.

APPENDIX 2 - Legal Considerations

There are a range of statutory provisions that impact on the use and disclosure of confidential information. These include but not limited to:

- **Common Law Confidentiality**: this is built up from case law where practice has been established as a result of individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider or with their subsequent permission.

- **Data Protection Act (DPA) 2018**: governs the processing (which includes holding, obtaining, recording, using and disclosing) of information. It applies to all forms of media, paper, images, data, etc.

- **The Human Rights Act (1998):** Article 8 of the act establishes a right to 'respect for private and family life' and this underscores the duty to protect privacy of individuals and preserve the confidentiality of their healthcare records. Other elements of the Act mean that any other legislation must be compatible. The DPA and Common Law Confidentiality satisfy this. In relation to disclosure and Article 8 – it must be justified as being necessary to support legitimate aims and be proportionate to need.

- **The General Data Protection Regulations (May 2018).**

Other key texts that support the safe, ethical and legal application of the law relating to confidentiality include the Confidentiality: NHS Code of Practice and the Caldicott Principles (which support day to day implementation of good practice when using and sharing confidential information).

- **The Caldicott Principles:**
  - Justify the purpose (of sharing information).
  - Don't use patient identifiable information unless it is absolutely necessary.
  - Use the minimum necessary patient identifiable information
  - Access to patient identifiable information should be on a strict need to know basis.
  - Everyone should be aware of their responsibilities.
  - Understand and comply with the law.
  - The duty to share information can be as important as the duty to protect patient confidentiality.

APPENDIX 3 - Systems and processes for protecting personal information

1. Thames Hospice uses both paper and IT based healthcare records and other patient service related databases.

2. Thames Hospice also has other databases used in connection with Fundraising, Retail, HR and other organisational and operational activities.

3. In order to ensure the safety of the data stored, each person who is granted access to the IT Network will be role assessed and given only the access they need to do their job. Each person will be given a personal log on and password, which must remain private to them and not shared. In some work areas there may be a shared log on to the whole system, but there are individual log on to specific databases (where there is shared responsibilities/care).

4. Passwords: each new user is issued a log on password which they are required to change immediately. Passwords should contain at least 8 characters, include at least one capital, one number or symbol and not be a word or name associated with the individual. Passwords will be changed every three months and cannot be repeated for at least 8 changes.

5. Staff are required to lock their computer when they leave their desk during the working day (Windows key +L) or (Control, Alt, Delete). When leaving the office for the day, staff must log off their computer and shut it down.

6. Smartcards: Clinical Staff issued with Smartcards are required to ensure they are kept on their person at all times and are not 'loaned' to anyone else. A separate policy determines correct use and management of smartcards at Thames Hospice.

7. Certain staff are able to access Thames Hospice's IT systems from mobile computers, etc. This remote access includes access to Patient systems where appropriate.

8. Thames Hospice email addresses should not be used to send or receive patient data as they are not encrypted.

9. Telephones and Faxes: staff are required to take into consideration the principles of the Caldicott Guidelines and the Data Protection Act when using telephones and/or faxes to share information. See guidance sheets:

    - Sharing Personal Information by Fax.
    - Sharing Personal Information by Phone.
    - Sharing Personal Information by Post.
    - Transporting Personal Information.

10. Hard Copy Records: All paper records generated by Thames Hospice will be managed in a confidential manner. They will be stored in a secure environment when not in use.

11. For clinical records:

    - An archive tracing process is in place to identify which department or staff member is responsible for them at any one time.
    - Individual records must not be left in public areas or unlocked office spaces unattended.
    - Staff must ensure the security of written patient information at all times.
    - Letters sent related to healthcare should be marked 'Private & Confidential – for Addressee Only' and sent in a securely sealed envelope.
    - If patient notes are required to be sent through the post should be marked Private and Confidential and should be sent recorded delivery or sent by hospital or other approved courier. A record of posting must be kept.

12. Paper Notes in the Community: Staff working in the community setting may need to take notes with them for their consultations. This should be with the approval of their manager and should be recorded as taken and returned. These should be in a sealed container/envelope and be stored in the boot of the car. Notes must not be left in cars unattended and, if taken home overnight, must not be left in a way that anyone other than the staff member responsible for them might see them. Total responsibility for the security of the notes lies with the individual who signed them out.

13. Electronic Notes in the Community: Community Staff are provided with appropriate training and encrypted laptops with which to access patient systems.

14. Thames Hospice will agree and record data sharing protocols with any external organisations with whom we regularly have a need to share information.

<u>Using and Disclosing Confidential Information – Deceased patients</u>

1. The use and disclosure of confidential information must be both lawful and ethical. Sometimes the law and ethics do not sit in parallel. The Department of Health and the General Medical Council agree that the principles of the Data Protection Act must continue to apply after death. Thames Hospice will continue to follow the principles of confidentiality in relation to deceased patient data and any requests to access this data.

APPENDIX 4 - Confidentiality Dos and Don'ts

DO

- 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 on or behalf of NHS England.
- Do 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.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do 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.
- Do share only the minimum information necessary.
- Do 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 or to a secure government domain e.g. gsi.gov.uk.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient identifiable.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

DON'T

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.