Access to Health Records Policy and Procedure (including general Subject Access Requests)

Approved by: Candy Cooley
Originator: Libby Mytton, Director of Care
Date of approval: November 2016

1. Introduction

The Data Protection Act 1998 (DPA) governs access to the health records of living people, and applies equally to health records held by the NHS and voluntary sector organisation such as Primrose Hospice. Subject to the conditions explained in this policy, individuals have the right to apply for access to health records irrespective of when they were complied.

Primrose Hospice also holds personal data in relation to staff, volunteers and donors, and follows the Subject Access Code of Practice: dealing with requests from individuals for personal information (ICO 2014).

2. Purpose of Policy

The Data Protection Act 1998 sets out certain restrictions on the extent and circumstances under which people can access information that is recorded in their health records and the purpose of this policy is to set out a clear set of instructions for staff to follow, to ensure that all requests are handled appropriately, in line with legislation and in a uniform manner.

Section seven of the DPA provides individuals with the right to find out what personal data an organisation holds about them, why the organisation is holding it and to whom it might be disclosed.

3. Definitions

For the purposes of the Data Protection Act 1998 (DPA), a health record is a record which:

- Consists of information relating to the physical or mental health or condition of an individual; and
- Has been made by or on behalf of a health professional in connection with the care of that individual.
Personal data must relate to a living individual and allow that individual to be identified from it (either on its own or alongside other information likely to be in the organisation’s possession).

*(Information Commissioner’s Office (ICO) 2014)*

Health records at Primrose Hospice include:

- the SystmOne (electronic) record
- paper records, including counselling and complementary therapy records

Personal data at Primrose Hospice will include:

- staff personnel files
- volunteer files
- donor details

4. Roles and Responsibilities

Management Responsibilities

Chief Executive

The Chief Executive is responsible for determining the governance arrangements of the Hospice including effective risk management processes. They are responsible for ensuring that the necessary clinical policies, procedures and guidelines are in place to safeguard patients and reduce risk. In addition they will require assurance that clinical policies, procedures and guidelines are being implemented and monitored for effectiveness and compliance.

Director of Care

The Director of Care has overall responsibility for patient safety and ensuring that there are effective risk management processes within the Hospice that meet all statutory requirements and adhere to guidance issued by the Department of Health.
Caldicott Guardian

The Caldicott Guardian has overall responsibility for the safety of patient and service user confidentiality and information sharing issues and has a key role in ensuring that the rules on confidentiality and information sharing are appropriately reflected in organisational policies and working procedures. At Primrose Hospice the Caldicott Guardian is the Director of Care.

The ‘Data Controller’

Under the DPA, responsibility for providing access to records lies with the ‘data controller.’ This is usually the health professional responsible for the patient’s care and at Primrose Hospice it will be the Director of Care.

Line Managers

Line managers are responsible for ensuring that:

- This policy is made available to all staff within their department
- The staff they are responsible for implement and comply with the policy
- That staff are updated with regards to any change in the policy

5. Procedure: Health Records and other SARs

Who may apply for access?

1. Health Records
   - Competent patients

   Competent patients may apply for access to their own records, or may authorise third parties such as lawyers, employers, or insurance companies to do so on their behalf. Patients at Primrose Hospice are informed of their rights to access their health records in a written leaflet entitled Worcestershire Palliative Care Services, provided on admission to services.
- **Individuals on behalf of those who lack capacity**

Patients with mental disorders or learning disabilities should not be automatically regarded as lacking the capacity to give or withhold consent to disclosure of confidential information. Unless unconscious, most people suffering from a mental impairment can make valid decisions about some matters that affect them. A person’s mental capacity must be judged in relation to the particular decision being made. If a patient has the requisite capacity, requests for access by relatives or third parties require patient consent.

When patients lack mental capacity, health professionals are likely to need to share information with any individual authorised to make proxy decisions. The Mental Capacity Act contains powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults, and the Court of Protection can also appoint deputies to do so. This may entail giving access to relevant parts of the incapacitated person’s medical record, unless health professionals can demonstrate that it would not be in the patient’s best interests. These individuals can also be asked to consent to requests for access to records from third parties. Where there are nominated individuals, requests for access to information relating to incapacitated adults should be granted if it is the best interests of the patient. In all cases, only relevant information should be provided.

- **Next of kin**

There is no definition or formal legal status to the term next of kin. A next of kin cannot give or withhold their consent to the sharing of information on a patient’s behalf. A next of kin has no rights of access to medical records.

- **Police**

If the police do not have a court order or warrant they may request voluntary disclosure of a patients’ health record under section 29 of the DPA. However, while health professionals have the power to disclose records to the police, there is no obligation to do so. In such cases health professionals may only disclose information where the patient has given consent or there is an overriding public interest. Disclosures in the public interest are made where disclosure is essential to prevent a serious threat to public health, national security, the life of the individual or a third party, or to prevent or detect serious crime.
• Solicitors

Health professional releasing information to solicitors acting for their patients should ensure that they have the patient’s written consent to disclosure and, where there is any doubt, confirm that the patient understands the nature and extent of the information disclosed. In practice, most solicitors will provide the patient’s signed consent when requesting confidential information.

2. General SARs

• Any individual may request information that he or she is entitled to ask for under Section 7 of the Data Protection Act 1998
• A third party such as a solicitor may make the SAR on behalf of a person, in which case the Hospice must be satisfied that the third party is in fact entitled to act on behalf of the person

When should access be given?

There is nothing in the law that prevents health professional from informally showing patients (or their proxies) their records as long as no other provisions of the Act are breached.

However, health professionals may supply copies of records only if a formal application for access to the records has been made.

Requests for access must be made in writing or electronically to the Director of Care. Once the written request has been received, the individual must be advised of the relevant fee (if any) and copies supplied to them promptly, and in any event, within 40 days. Sometimes additional information is needed before copies can be supplied and in such cases the 40 day time limit will begin as soon as the additional information has been received.

A record will be kept of the timeline, starting on the date the request was received and including all significant dates thereafter.

For how long is a patient’s written consent valid?

There is no time limit after which consent for disclosure of information becomes invalid. However, if there has been a significant interval between the time the patient signed the letter of form and its receipt, it would be good practice for the health professional to contact the patient to confirm that he or she is still willing to agree to the disclosure, particularly if it is to a third party such as a solicitor or insurance company.
Fees

Requests for fees, particularly where a third party is requesting access to records, may, entirely at the discretion of the Hospice, be charged in line with the ICO code of practice as follows:

<table>
<thead>
<tr>
<th>Fees for copies of health records of living patients</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records kept on a computer</td>
<td>Up to a maximum of £10</td>
</tr>
<tr>
<td>Health records held in part on a computer and in part manually</td>
<td>Up to a maximum of £50</td>
</tr>
<tr>
<td>Health records held manually</td>
<td>Up to maximum of £50</td>
</tr>
</tbody>
</table>

Fees to allow patients access to their own records where no copy is required:

| Health records held totally on computer             | Up to a maximum of £10 |
| Health records held in part on computer and in part manually | Up to a maximum of £10 |
| Health records held manually                        | Up to a maximum of £10 unless the records have been added to in the last 40 days in which case viewing should be free |

When should information not be disclosed?

Information should not be disclosed if:

- It is likely to cause serious physical or mental harm to the patient or another person
- It relates to a third party who has not given consent for disclosure (where that third party is not a health professional who has cared for the patients)
- It is requested by a third party and the patient has asked that the information be kept confidential
- The records are subject to legal professional privilege, which may arise in the case of an independent medical report written for the purpose of litigation

The data controller should redact, or block out any withheld information, and must be prepared to justify the decision to do so. The data controller may advise patients of the grounds on which information has been withheld but is not obliged to do so. There is still an obligation to disclose the remainder of the record.
The Data Controller (Director of Care) may consult members of the multi-disciplinary team who best know the patient for advice relating to serious harm.

Circumstances in which information may be withheld on the grounds of serious harm are extremely rare, and this exemption does not justify withholding comments in the records because patients may find them upsetting.

**Can patients read their records if they do not request copies?**

The DPA does not expressly allow patients to read their records where no copy is required, although they are permitted to do so with the agreement of the data controller.

**Supporting patients who are reading their records**

Patients may become distressed whilst reading their records and it is advisable for a member of staff to provide or offer support. The DPA requires that the information supplied to an individual is in an intelligible form, and an explanation of any medical terms or jargon may be required.

**Health Records of DeceasedPersons**

Access to the health records of a deceased person is governed by the Access to Records Act 1990 (AHRA).

This act provides certain individuals with a right of access to the health records of a deceased person. These people are defined as:

- The patient’s personal representative
- Any person who has a claim arising out of the person’s death

The personal representative is the only person who has an unqualified right of access to a deceased person’s record and need give no reason for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient’s death.

It is essential to ascertain the status of the applicant to ensure that the requestor is a bona-fide person as described in the AHRA, also to understand the details of any alleged ‘claim’ prior to disclosure of any part of the health record.

No other information than that which is directly relevant to a claim should be disclosed to either the personal representative or any other person who may have a claim arising out of the person’s death.
An application for access will be made to the Data Controller (Director of Care) who will need to take advice, including legal advice, prior to making a decision about disclosure.

Information that may be released under this legislation is limited to health records and not any other information about the deceased, and any proposed disclosure would need to be examined closely to ensure that any non-medical information is carefully redacted.

Access can be given by allowing the applicant to inspect the records or extract or by supplying a copy if requested.

Where the application concerns access to records, or parts of records made in the 40 day period immediately preceding the date of application access must be given within 21 days.

Where the access concerns information all of which was recorded more than 40 days before the date of the application, access must be given within 40 days.

Information should not be disclosed if:

- It identifies a third party without that person’s consent unless that person is a health professional who has cared for the patient, or
- In the opinion of the relevant health professional, it is likely to cause serious harm to a third party’s physical or mental health, or
- The patient gave it in the past on the understanding that it would be kept confidential. No information at all can be revealed if the patient requested non-disclosure.

6. Review

This policy will be reviewed every 3 years, or sooner if local or national guidance or legislation requires.

7. Policy Area

Information and Research.

8. Staff Training Requirements

Staff will be made aware of this policy at induction. More specific training on SARs, how to recognise them and how to process them will be provided as part of Information Governance training.