Mid Essex Hospital Services NHS Trust

| | |
|---|---|
| **ACCESS TO RECORDS POLICY** | **Policy**<br>**Register Number: 04086**<br>**Status: Public when ratified** |

| | |
|---|---|
| Developed in response to: | General data Protection Regulation (GDPR) Guidance |
| CQC Fundamental Standard: | 17 |

| **Consulted With:** | **Post/Committee/Group:** | **Date:** |
|---|---|---|
| Martin Callingham | Chief Information Officer | May 2018 |
| Goolam Ramjane | Information Governance Manager | May 2018 |
| Helen Clarke | Head of Governance | May 2018 |
| Liz Stewart | Co-Public Information Manager | May 2018 |
| Vicki Chapman | Health Records Manager | May 2018 |

| **Professionally Approved by:** | | |
|---|---|---|
| James Day | Trust Secretary | June 2018 |

| | |
|---|---|
| Version Number | 6.1 |
| Issuing Directorate | Corporate/Information Governance |
| Ratified on | 29th June 2018 |
| Ratified by | DRAG Chairman's Action |
| Trust Executive Sign Off date | July 2018 |
| Implementation Date | 2nd July 2018 |
| Next Review Date | May 2021 |
| Author/Contact for Information | Rebecca Pascoe-Youell, Public Information Manager |
| Policy to be followed by (target staff) | All Trust Staff |
| Distribution Method | Intranet Trust website |
| Related Trust Policies (to be read in conjunction with) | Confidentiality Policy<br>Information Governance Policy<br>Sending Trust Information out of the UK<br>Data Protection Strategy<br>Incident Policy |

**Document Review History:**

| **Review No:** | **Reviewed by:** | **Issue Date:** |
|---|---|---|
| 1.0 | Liz Stewart | January 2004 |
| 2.0 | Karen Hull | September 2005 |
| 3.0 | Liz Stewart | February 2007 |
| 4.0 | Liz Stewart | February 2010 |
| 5.0 | Liz Stewart | March 2014 |
| 5.1 | Liz Stewart - Extension agreed to December 2018 due to review of GDPR | 27th February 2018 |
| 6.0 | Rebecca Pascoe-Youell | 2nd July 2018 |
| 6.1 | Rebecca Pascoe Youell - removal of section entitled viewing records; update Appendix 1. | 15th March 2019 |

**Index**

## 1.0 Purpose

1.1 The purpose of this policy is to define the Trust's response to requests for access to records from a patient, their relatives or a third party legal professional for litigation purposes. It also includes access to records by other NHS or non-NHS clinical care providers and to records required for Research and Audit purposes.

1.2 It also defines the responsibilities of the Human Resources and Occupational Health Departments in relation to requests for access to personal records by staff.

1.3 This policy reflects various current legal and professional guidelines and places controls that meet the needs of:

- General Data Protection Regulation (GDPR)/UK Data Protection legislation
- Access to Health Records 1991
- Subject Access Code of Practice – Information Commissioners Office 2013

## 2.0 Scope

2.1 A health record for the purposes of the data protection legislation is a recording which relates to the physical or mental health of an individual made in connection with the care of that individual.

2.2 A health record is defined as being any data or image held in any media that provides information about a patient. It therefore includes:

- Paper records, both current, archived or overflow volumes
- Data on microfilm
- Digitally held archive
- Any imaging media, radiographic, photographic or televisual
- Emergency attendance records
- Therapy records
- EEG/ECG traces
- Information held on any Trust clinical system
- Information held on any register that has not been transferred to the Essex Records Office

2.3 Staff Records are provided for under the data protection legislation and these can include:

- Personal file
- Occupational health records
- Emails and other correspondence relating to the requester that constitutes "personal data" under the data protection legislation , however not all correspondence that may relate to the requester is disclosable, for example, if it would identify a third party who had not given their consent to the disclosure.
- CCTV images are excluded from routine disclosure because they usually include images of other patients, staff and visitors. These would be subject to a decision on a case by case basis.

2.4 This policy excludes:

- Duplicate records provided to other health care providers.

- Duplicate individual letters provided directly to patients by consultants/medical secretaries in line with the “Copying Letters to Patients” government objective.
- Medical reports that are completed by consultants for the benefit of the courts, insurance companies and the Police.
- Access to data that is anonymised. The Trust will manage requests for anonymised or pseudonymised information under the Freedom of Information Policy.
- The provision of original records for court purposes, however the Trust will take a paper copy of these records prior to their release. The Access to Records Bureau only may undertake this task.
- Adopted children with new names are outside the scope of this policy. There is one national register of old and new names of adopted children held by the Department of Health to whom these adopters will need to apply.

## 3.0 Policy Statement

3.1 It is not the intention to unreasonably withhold access to records. The policy enables access to those who require information whilst ensuring that essential safeguards are in place to protect patient information from inappropriate or illegal requests.

3.2 The General Data Protection Regulation became law in May 2016 and came into force in May 2018.

3.3 The GDPR introduces a principle of ‘accountability’. This requires that organisations must be able to demonstrate compliance. Some of the key obligations to support this policy include:

- The recording of all data processing activities with their lawful justification and data retention periods.
- Ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights.
- Ensuring that data subjects’ rights are respected
  (the provision of copies of records free of charge, rights to rectification, erasure, to restrict processing, data portability, to object and to prevent automated decision making).
- Notification of personal data security breaches to the Information Commissioner.
- The appointment of a suitably qualified and experienced Data Protection Officer.

3.4 The GDPR gives an individual several rights in relation to the information held about them. Access covers the right to obtain a copy of the record in permanent form, unless the supply of a copy would involve disproportionate effort or the individual agrees that his/her access rights can be met some other way. Access must be given promptly within 30 days (calendar month) of receipt of the application and verification of the identity. If the application does not include sufficient details to identify the person making the request or to locate the information, those details should be sought promptly and the 30 day period begins when the details have been supplied.

3.5 This right of access is only exercisable by the individual; making a written application to the organisation holding the records, providing such further information as the organisation may require to sufficiently identifying the individual.

However the Information Commissioners Office has defined, through case law, that the information relating to the deceased should be protected in the same way as that of the living.

## 4.0 Rights of Access

4.1 Subject Access is most often used by individuals who want to see a copy of the information an organisation holds about them. However subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people.
- Given a copy of the personal data.
- Given details of the source of the data.

4.2 Subject Access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. There is therefore no obligation to supply copies of original documents.

4.3 Most personal data, however stored, falls within the scope of the General Data Protection Regulation (GDPR)/UK Data Protection legislation to which the Data Subject (patient or staff member) or legal representative has access and that access applies to all Trust held records that constitute "personal data" and are within their retention period. But there are some exceptions. Records will not be supplied if:

- It is not possible to identify the data requested from the information provided.
- If the information given about the proof of the identity of the enquirer is insufficient.
- Where disclosing the personal data would reveal information that had been provided by a third party with the clear expectation that it would never be passed on to the data subject.
- Where having all or some of the information is not in the best psychiatric interests of the patient or member of staff. This decision will always be taken in conjunction with the treating clinicians, but the expectation will be that the information will be supplied unless there is an overwhelming reason not to do so. But this is not a "forever" decision as it might be decided just to postpone the disclosure pending an improvement in the a patient's mental wellbeing and in these the cases the treating clinicians will officially write to the patient explaining the decision and there should be a copy of the this letter placed in the patient's medical record.

4.4 In disputed cases, the disclosure decision will be taken by the Trust's Data Protection Officer who if necessary will consult the relevant health and legal professionals and with the Information Commissioners Office.

4.5 There are also a range of public bodies that have lawful authority to require the disclosure of health information. These include the Courts, legally constituted Public Enquiries and various regulators and commissioners e.g. the Care Quality Commission. In these cases the common law obligation to confidentiality is overridden.

## 5.0 Access to Deceased Records by a Third Party

5.1 The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under Section 3(1)(F) of that Act as, 'the patients' personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the Executor or Administrator of the deceased person's estate. Apart from statutory bodies, only the deceased patient's legitimate and legal representative has a statutory right to have a copy of the medical records. They do not need to state

why they are making the request but they do need to provide evidence that they are the legal representative.

5.2 Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis. The public good that would be served by disclosure must outweigh both the obligation of confidentiality owed to the deceased individual and any other individuals referenced in a record.

5.3 Key issues for consideration include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. The views of surviving family and the length of time after death are also important considerations. The obligation of confidentiality to the deceased is likely to be less than that owed to living patients and will diminish over time.

5.4 Another important consideration is the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information abstracted from the records. If the point of interest is the latest clinical episode or cause of death, then disclosure, where this is judged appropriate, should be limited to the pertinent details.

5.5 Individuals requesting access to a deceased patient's health information should be able to demonstrate a legitimate purpose, generally a strong public interest justification and in many cases, a legitimate relationship with the deceased patient. On making a request for information, the requester should be asked to provide authenticating details to prove their identity and their relationship with the deceased individual. They must also provide a reason for the request including explaining to the satisfaction of the Trust that they have a claim arising out of patient's death if they are not the Personal Representative. Where possible they should specify the parts of the deceased health record they require for the reasons outlined in 5.4. If a request is turned down because the Trust believes that the request is not valid, the requester has a right of complaint to the Information Commissioners Office.

5.6 Relatives, friends and carers may not qualify to have copies of medical records but still have a range of important and valid reasons for requesting information about deceased patients. For example, talking to relatives to help them understand the cause of death and actions taken to ease suffering of the patient may help aid the bereavement process and these conversations should still take place irrespective of their legal rights to copy documentation.

## 6.0 Fees Payable

6.1 No Fee is payable for a Subject Access Request unless the request is deemed manifestly unfounded or excessive, in which case a reasonable fee may be chargeable.

6.2 Fees, if charged must be received by the Trust prior to work commencing on collation of the records.

6.3 Where solicitors require more copies of photographs that the one copy that is legally required to be provided, the solicitors will deal with the Medical Photography Department direct for the additional copies, however the additional fees will be paid in to the one centrally held budget for all duplicate records NABD 1W02. The fees for additional copies are outside the scope of the Data Protection regulations, so the Trust may charge whatever it considers reasonable for this service.

## 7.0 Overview of Procedure

7.1 The Access to Records Bureau logs requests and releases all copy records except those released by the Complaints Department, Claims Manager and Trust Secretary. Other Trust staff are not permitted to provide duplicate records under the Act.

7.2 All records will be released by Access to Records without reference to any clinical view other than the situation already explained in 4.3 last bullet point. This is on the basis that within acute healthcare records there should not be anything recorded that is not releasable.

7.3 Solicitors may apply by letter but must supply an applicant signature on appropriate documentation although this now may be either an original or an electronic signature. Electronic signatures will not be accepted by any requesters other than solicitors.

7.4 A request for copy records must be responded to within 30 days.

7.5 If the requester is outside of EEA (European Economic Association) it is necessary to inform the requester that the Trust cannot guarantee the security of manual or electronic data transfer and they will have to confirm in writing that they consent to accept the risk. Refer to the Trust's Sending Information out of the UK Policy for more information.

7.6 All radiographic data that is downloaded from PACS and issued as a duplicate record under the data protection legislation will be encrypted in line with Department requirements. However it is understood that in some circumstances, usually relating to organisations with complex IT networks in terms of security, that the encrypted discs will not open. In these circumstances it is necessary to provide discs unencrypted, however encryption is the default position.

## 8.0 Children's Records

8.1 For the purposes of disclosure a child is a person who has not attained their 16th birthday. If the applicant is 16 or over they should be treated in the same way as an adult. The parents or guardians of the applicant over 16 years are not entitled to see the records without the consent of the young person. The only exception to this is when the child lacks capacity and the parents or guardian hold a Lasting Power of Attorney.

8.2 If the application is by a data subject who is under 16, the Trust will need to obtain parental authority on the basis that an applicant under 16 is not authorised to make a request under the General Data Protection Regulation (GDPR)/UK Data Protection legislation. However the Trust will look sympathetically at a request from a child aged in between 12-16 who is judged to be "Gillick Competent" but any release will be authorised by the child's treating consultant based on the perceived maturity of the individual and the situation that pertains at the time. Decisions will be made only on a case by case basis.

## 9.0 Adult requesters without Capacity

9.1 The General Data Protection Regulation (GDPR)/UK Data Protection legislation makes no special provisions about requests for access on behalf of an adult who lacks mental capacity and is incapable of managing their own affairs.

9.2 Mental disorder does not equate with mental incapacity and many persons suffering from a mental disorder have sufficient capacity to enable them to deal with their own affairs. The patient's clinician(s) will make a decision, if necessary in conjunction with their colleagues within mental healthcare, about the appropriateness of releasing records.

9.3 Patients with learning difficulties, depending on their individual circumstances may have enough capacity to understand the process, albeit with support. The Hospital Liaison Specialist Nurse, Learning Disability Lead, will advise in these situations.

9.4 Patients with learning disabilities who do not have capacity should have an MCA2 form in their medical records. Any requests from such a patient should be referred initially to the Trust's Adult Safeguarding Lead.

## 10.0 Requests by the Police

10.1 It is important that all staff are aware that only the Access to Records Bureau discloses health records to the Police unless the Police provide the relevant Exemption form, usually referred to as their A101 form.

10.2 In the event that the Police request staff records, including Occupational Health Records, these will only be provided to the Police by a senior member of the HR Team, again on the production of an A101 form.

10.3 The A101 form must be fully completed in order to be valid. It must contain an explanation of why the information is required and be signed by a more senior officer than the officer requesting.

10.4 All email communications with the Police must be sent on nhs.net accounts to a secure email address that includes pnn.police in the title.

10.5 In the event of telephone calls from the Police, their identities must be verified before any information is provided. Staff should ask for the name of their force eg Essex Police/Metropolitan Police and their extension number that can be reached via phoning 101. Staff must not accept a number from a mobile or ring back a mobile until after communications have been set up via a 101 number and officers become individually recognisable.

10.6 Police will attend the hospital soon after an admission of an injured victim (or assailant) and will need certain information to provide to magistrates courts that may well be taking place the following day. In these instances, they will require Medical Statements which must be given by a member of the clinical staff, but these do not constitute "health records". The need for police to have copies of the medical records is usually much later on and that is the process managed by the Access to Records Bureau. But as set out in 10.3, if the police are in attendance in clinical areas and asking for copies of any part of the medical record, then they must provide an A101 form.

10.7 In the event that any member of the Police demands copies of medical records without an A101, particularly out of hours, the Trust understands that staff can feel very intimidated and might be inclined to hand over the documentation just to have the Police leave the clinical area particularly late in the evening or at night. In this circumstance, staff should call the Bed Office for assistance. Staff will not be d blamed if they were in a genuinely difficult situation and support was not available.

10.8 All attempts by the Police to obtain information inappropriately must be recorded on Datix. These will all be reported to the Chief Superintendents of the relevant police force.

## 11.0 Records Required as Evidence for Investigatory or Disciplinary Processes

11.1 Staff who are under investigation or are subject to disciplinary proceedings may require access to information that is held in patient health records because either:

- they recorded it and need to provide it as evidence or
- there are entries made by other staff that support their case

11.2 In these cases, staff will only have access to the elements of the records that they need and any access will be supervised either by the Access to Records Bureau or by HR Department staff.

11.3 Staff will only be able to have photocopies of the material specified in 11.1 and patient names will be redacted and replaced by hospital numbers before they are provided to the staff member. Staff are not permitted to retain any photocopied medical records beyond the end of the investigation/disciplinary/appeal event to which they pertain. The copied records must be confidentially disposed of at the earliest possible opportunity.

## 12.0 Requests to amend medical records after the Data Subject has received copies

12.1 Credible records are an important aid in providing safe healthcare to patients. Records should reflect the observations, judgements and factual information collected by the contributing health professional.

12.2 One of the data legislation principles requires that information should be factual and kept up to date. This provides the legal basis for enforcing correction of factual inaccuracies. An opinion or judgement recorded by a health professional, whether accurate or not, must be deleted. Retaining relevant information is essential for understanding the clinical decisions that were made and to audit the quality of care.

12.3 If a patient feels that information recorded on their health record is incorrect, they should first make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. Where both parties agree that information is factually inaccurate, it should be amended to clearly display the correction whilst ensuring that the original information is still legible. An explanation of the correction should also be added, signed and dated by the person making the correction.

12.4 Where the health professional and patient disagree about the accuracy of the entry, the Trust will allow the patient to include a statement within their records to the effect that they disagree with the content. This should be placed in a sealed envelope and filed in the correspondence section of their record. It should be marked on the front what the envelope contains and what date during their care it refers to. The section of the records to which the patient objects should be asterisked and a signed and dated statement placed adjacent to it, marked: - “the patient disagrees with this section and their comments are in a dated envelope and filed in the correspondence section.

12.5 There is only one scenario when an entry in a medical record can be obliterated and that is when it has been entered into the wrong patient’s record. If this occurs, the entry must first be replicated in the correct folder i.e. it must be entered as it was written and then checked that the wording is correct. After that, the recording in the wrong record

may be redacted. However a statement must be input next to the redaction, explaining that the entry did not refer to the patient named on the record. In this scenario it is acceptable for someone other than the staff who made the initial incorrect entry, to copy across that entry to the correct folder, but again, that entry must be fully explained, dated and signed.

## 13.0 Patients living abroad requiring access to their medical records

13.1 Former patients living outside the UK who had treatment in the UK and are now domiciled outside of the EEA, have the same rights under the data protection legislation to apply for access to their UK medical records. Similarly, ex member of staff who may move or retire abroad retain the right under the data protection legislation to access their employment records.

13.2 Original records must not be given to patients to keep or take to a new GP abroad. In instances when a patient moves abroad a GP may be prepared to provide the patient with a summary of their treatment. Alternatively, the patient is entitled to make a request for access under the data protection legislation to obtain a copy.

13.3 If the former patient resides in a country outside of the EEA, the Trust must comply with the GDPR/UK data protection legislation that requires that person identifiable information should not be transferred out the EAA. In these situations, the patient must not only make the request but issue explicit informed consent that they understand that there is a security risk in transferring the data, both manually and especially electronically.

## 14.0 Non-Compliance with this Policy

14.1 Any non-compliance with this policy must be recorded on Datix and fully investigated and reported in accordance with the Incident Reporting Policy.

## 15.0 Audit & Monitoring

15.1 Breaches of this policy that are categorised as breaches of confidentiality will be recorded on Datix.

## 16.0 Communication & Implementation

16.1 This policy will be uploaded to the intranet and Trust website and will be communicated to staff via internal newsletter.

16.2 Individual copies will be emailed to each member of the Access to Records Team, the Trust Secretary and Head of Complaints.

## 17.0 References

Subject Access Code of Practice, Information Commissioners Office, August 2013

Guide to the General Data Protection Regulation, Information Commissioners Office January 2018

Access to Records, Department of Health, updated February 2010

# APPLICATION FOR ACCESS TO HEALTH RECORDS

**(General Data Protection Regulation GDPR / UK Data Protection legislation / Access to Health Records Act 1992)**

**1. Patient Record to be accessed:**

| | |
|---|---|
| Surname (family name) | |
| First name (s) | |
| Date of Birth | |
| Hospital Number | |
| NHS Number | |
| Previous name or other names known by | |
| Address<br><br>Contact telephone number | (Provide previous address if applicable on separate sheet) |
| Email Address | |

**2. Details of Applicant (if you are NOT the patient listed in 1.):**

| | |
|---|---|
| Surname(family name) | |
| First name(s) | |
| Company name (if applicable) | |
| Address<br><br>Contact telephone number | |
| Email Address | |
| Relationship to Patient | |

**3. Your request – Records requested will be sent to you on CD by 2nd class post**
**Please tick one box to indicate where records should be sent to:**

| | |
|---|---|
| I am the patient and would like my records to be sent to my home address (in section 1) | |
| I am acting on behalf of the patient and would like the records sent to the address (in section 2) | |

**What do you want to receive? (* compulsory to complete)**

*** About what? (condition / illness etc)**

*** When? (date treatment received if known or approx)**

| | | | |
|---|---|---|---|
| Do you require X-rays / MRI / CT Scans | | Do you require Emergency Department (A&E) Records? | |
| Do you require physiotherapy records? | | Do you require photographs? | |
| Do you require pathology results? | | Do you require clinical notes? | |

***Please continue to complete page 2 of this request***

### *4. Declaration and consent to release records:*

***I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record referred above under the terms of the General Data Protection Regulation 2018. (See supporting evidence required eg A&B)***

| **Please Tick the appropriate box** | |
|---|---|
| I am the patient and applying for a copy of my own records **(A&B both required)** | |
| I am applying for the records of a child under 16 for whom I am the parent/guardian/ have parental responsibility, **(A,B&C all required)** | |
| I am the deceased person's legal representative and I attach evidence of that status **(A,B&C all required)** | |
| I am applying for the medical records of a deceased person and I am not their legal representative. Please provide evidence of your identity and relationship to the deceased person along with the reason for your request which needs to be a valid claim arising out of the patient's death. **(A,B&C all required)** | |
| I am acting on behalf of a consenting adult with capacity and attach their authorisation to release their records to me **(A,B&C all required)** | |
| I am the Executor of the Estate of the deceased person and attach evidence of my appointment as executor **(C)** | |
| Any other request not covered by the above, please provide relevant supporting information. | |

**I am the patient:**

| | |
|---|---|
| Name | |
| Signature | |

**I am acting on behalf of/or for the patient:**

| | |
|---|---|
| Name | |
| Signature | |

### 5. Supporting Evidence Required

The following identification evidence should be attached to this document – what you need to supply depending on your situation is detailed in 4. **For further detail about evidence to support your request please refer to the support information page accompanying this form**.

.

| **Supporting Evidence** | **Evidence Provided (please tick and detail)** |
|---|---|
| A. Evidence of confirmation of name: | (e.g. copy of passport) |
| B. Evidence of confirmation of address: | (e.g. copy of utility bill) |
| C. Evidence of Third Party confirmation (if Applicable): | (e.g. copy of health and welfare power of attorney) |

**Please send the completed form with evidence to the address beneath:**

**Access to Records Bureau R42, Mid Essex NHS Hospital Services Trust**
**Court Road, Chelmsford CM1 7ET**
Email:accesstorecordsbureau@nhs.net / Tel: 01245 514288

**Supporting Information concerning Evidence for Identification**

**Please be informed that you are required, as part of your application for access to medical records, to supply evidence to confirm your name, your address and your ability to access the records of the data subject. Please supply evidence, where indicated on section 4 of the application form, depending on your personal situation.**

**Evidence can be selected from the following lists:**

**A. Confirmation of name**

- Full driving licence
- Passport
- Birth certificate
- Marriage certificate / Civil Partnership Certificate
- HM Forces ID Card

**B. Confirmation of address**

- Utility bill (not older than 3 months)
- Bank statement (not older than 3 months)
- Council Tax Bill of the current year
- Mortgage statement of the current year

**C. Confirmation that a third party can access the records of the data subject**

- Health and Welfare Lasting Power of Attorney
- Full birth certificate of child
- Full marriage certificate of parents (if details not shown on birth certificate)
- Full certificate of adoption
- Parental Responsibility Order
- Signed declaration from the Data Subject themselves
- Court of Protection Order appointing you as a personal deputy for the personal welfare of the data subject
- Confirmation of appointment as Executor of Estate (Certified copy of Letters of Administration or Grant of Probate)

**The Access to Records function has 30 days to respond to your request.**

- ✓ **Have you completed the application form fully with all relevant information and contact details?**
- ✓ **Have you attached relevant evidence to support your application?**
- ✓ **Please contact us if you require records in a different format or you have any questions.**

**Please send the completed form with evidence to the address beneath:**
**Access to Records Bureau R42, Mid Essex NHS Hospital Services Trust**
**Court Road, Chelmsford CM1 7ET**
Email:accesstorecordsbureau@nhs.net / Tel: 01245 514288