South East Coast Ambulance Service NHS
NHS Foundation Trust

Data Subject Access Request Policy and Procedure

Contents

1 Introduction

1.1. The South East Coast Ambulance Service NHS Foundation Trust (the Trust) regards the Data Protection Act 2018 / UK General Data Protection Regulation as an important legislation mechanism in achieving a transparent and safe relationship with its patients and employees.

1.2. The Data Protection Act 2018 (the Act) / General Data Protection Regulation 2016 came into force on 25th May 2018. This legislation entitles an individual (with certain exceptions) to a copy of their personal data which is held in both manual (paper) and computer data format, that is held by the Trust.

1.3. They are also entitled to know how the data is captured, why it is processed and with whom it is shared.

1.4. A request for such information under the Act is known as a Data Subject Access Request (DSAR) and is represented under Article 15 of the UK General Data Protection Regulation – Right of Access.

1.5. Where individuals are applying for access to a deceased person's records the Access to Health Records Act 1990 applies.

1.6. The Trust receives requests for access to health records from patients; their relatives; solicitors pursuing civil claims; solicitors defending criminal prosecutions; the police; coroners; and insurance companies acting on behalf of patients. Equally, the Trust may also receive requests for access to personnel records from members of staff or others whose personal data we hold.

1.7. Data Subject Access Requests for Human Resources (personnel records) will be managed by the Human Resources Directorate.

1.8. Requests for health records made by patients or their relatives will be managed by the Patient Experience Team; and

1.9. Those from solicitors, coroners, the police or insurance companies will be managed by the Trust Legal Services Department.

2 Aims and Objectives

2.1. The aims of this policy and procedure are to:

2.1.1. Ensure that effective arrangements are in place concerning access to personal data; and

2.1.2. Ensure that disclosures of personal data are lawful and processed in accordance with relevant legislation.

3 Definitions

3.1. **Personal Data:** this relates to a living individual who can be identified :

3.1.1. From that data which is being held; or

3.1.2. From that data which is being held and other information which is in the possession of, or is likely to come into the possession of, the data controller; and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2. **Data Controller:** a person / organisation who (either alone or jointly or in common with other persons / organisations) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.3. **Data Subject:** an individual who is the subject of the personal data. A data subject must be a living individual. The data subject can be, but is not limited to:

3.3.1. An employee of the Trust

3.3.2. A patient or service user of the health services provided by the Trust

3.3.3. A member of the public included in CCTV footage

3.4. **Relevant filing system**: any set of manual or electronic information files relating to individuals that are structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

3.5. **Health Record:** a record made by, or on behalf of, a health professional in connection with the care of an individual. It must relate to the physical or mental health or condition of the individual and the data subject must be identifiable from the information in the

record or other information in the possession of the holder of the record.

3.5.1. Thus, if the reference is only identified by a number or other reference, but the holder has information that can be used to identify the individual from the reference, the information is a health record as defined under Legislation.

This also covers photographic or graphical records such as x-rays, ultra sounds, computer generated information, ECGs, video tapes, etc.

3.6. **Health Professional**: a health professional is defined in the Act as:

3.6.1. A registered medical practitioner

3.6.2. A registered dentist

3.6.3. A registered optician

3.6.4. A registered pharmaceutical chemist

3.6.5. A registered nurse, midwife or health visitor

3.6.6. A registered osteopath

3.6.7. A registered chiropractor

3.6.8. Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends

3.6.9. A clinical psychologist, child psychotherapist or a speech therapist

3.6.10. A music therapist employed by a health service body

3.6.11. A scientist employed by such a body as a head of a department

3.7. **Right of Subject Access:** an application for a Data Subject Access Request may be made by:

3.7.1. **The Data Subject:** the individual who is the subject of the data is entitled to ask to see or receive a copy of any data about themselves

3.7.2. **On behalf of the Data Subject:** a third party applying for Data Subject Access Request with the consent of the data subject.

3.7.3. **A Person with Parental Responsibility:** someone with parental responsibilities (if a guardian or grandparent or another holds parental responsibility they will need to present the legal evidence) can submit a data subject access request on behalf a child.

3.7.3.1 However, if the child is at an understandable age (the law regards young people of 16 or 17 to be adults for the purposes of consent to treatment and right to confidentiality), then the child must give written consent to the person with parental responsibilities for them to access the information on their behalf or make the application personally.

3.7.3.2 The relevant Health Professional may decide that parental access is not in the child's best interests.

3.7.4. **A Person appointed by the Courts:** where a patient is incapable of managing their affairs, someone appointed to act on their behalf by a court of law may submit a data subject access request. Proof of the court order must be given.

3.7.5. **Lawyers acting on behalf of a Client or Insurance Companies:** where a solicitor, lawyer or other legal professional requests access on behalf of a client they are representing, the signed consent of their client must be obtained and evidenced. The request must be dealt with in the same way as if it had come direct from the data subject.

3.7.6. **Other Agencies:** in some circumstances the Trust may be asked to provide information to other agencies. Unless there is a legal requirement to disclose, the data subject must be informed and their consent obtained in writing.

3.7.7. Where there is a legal requirement to disclose, consent does not need to be sought, but the data subject must be informed in writing of the disclosure.

3.7.8. **A Family Member or Appointed Representative of a Deceased Data Subject:** Under the Access to Health Records Act 1990 a request to see a deceased patient's health record or to have a copy thereof can be made by the patient's personal representative or any person who may have a claim arising out of the patient's death. These are the only cases where access to the deceased's health records may be given.

3.7.9. Applicants in respect of deceased patients are entitled to information held in manual records from 30/10/1991 unless records prior to that date are needed to ensure an understanding of the subsequent records. Computerised data can be obtained from 1984 onwards.

3.8. **Application Process:** the application for a Data Subject Access Request must be made in writing. No reason need be given. Patients may verbally request access to their records and in many cases this can be dealt with informally. These verbal requests will not be applications under the Act. Information disclosed in an informal request must only be disclosed with the consent of the professional who created the data.

3.9. **Records held by a Third Party:** applications received requesting access to files or records that are not held or were generated by professionals who were not employed by the Trust at the time of making the record cannot be dealt with and the applicant will be referred to the agency holding the record if known.

3.10. **Head of Information Governance :** Information Governance Manager.

3.11. **Caldicott Guardian:** each NHS organisation has to have a Caldicott Guardian who should be, in descending order of priority: an Executive member of the Board; a senior health or social care professional; and responsible for clinical governance.

3.12. The Caldicott Guardian promotes patient interests and their confidentiality at Board level and is responsible for enabling appropriate information sharing in line with legislation.

4 Policy Statement

4.1. The Trust is committed to facilitating appropriate access to personal data for its employees, patients and other stakeholders.

4.2. Data Subject Access Requests can be made verbally, in writing or via email with evidence of identity provided to the satisfaction of the Trust.

5 Arrangements

5.1. Verbal Informal Application

5.1.1. This shall be dealt with locally and is down to the discretion of the professional who created the record. Any information disclosed must be recorded on the data subject's file, whether it is a health record or a personnel staff file.

5.1.2. A verbal application is not a data subject access request under the Act. If the data subject has any dispute about the information disclosed, that cannot be resolved, then a formal application must be made by them in writing as below.

5.2. Receipt of Application

5.2.1. Under the DSAR provision individuals can make a request verbally or in writing. This includes e-mail either from the data subject themselves or from someone who has the right of access to that record or has the data subject's written permission.

5.2.2. All applications will be passed to either:

5.2.2.1. the Complaints/PALS Officers (requests for access to health records from patients or their relatives; or

5.2.2.2. the Trust Legal Administrators (requests for access to health records from the police, coroners, solicitors or insurance companies; or

5.2.2.3. HR Business Managers (requests from staff for access to personnel records)

5.2.3. In all cases details of the request will be recorded on the locally held Data Subject Access Request database.

5.2.4. When a data subject access request is received the above staff will, where necessary, write to the applicant to gain all the necessary information e.g. proof of identity or obtain signed consent.

5.3. All application documentation must be date stamped on receipt. The applicant has a right to a permanent copy of their entire record but may not require this. Where it is unclear, confirmation of what material is required must be obtained to ensure an appropriate response.

5.4. **Validity of Application**

5.4.1. The person handling the request must be satisfied as to the identity of the applicant to determine their entitlement to receive the information requested.

5.4.2. Examples of proof would normally be either a photocopy of a passport, birth/marriage certificate or driving licence and recent utility bill. However, requests from staff who are known to the member of staff handling the enquiry may be made using their 'secamb' email address.

5.4.3. If the application for access to a child's records is made by someone having parental responsibility access shall only be given when:

5.4.3.1. The child is capable of understanding what the application is about and has consented to it; or

5.4.3.2. The child is not capable of understanding the nature of the application and giving access would be in his/her best interests.

5.4.4. The Caldicott Guardian will decide on the child's capacity to understand the application.

5.4.5. The request may be refused if information that is reasonably required to identify the person making the request, including any third party authority, and to locate the information required, is not made available.

5.5. **Administration**

Applications can be divided into three groups:

5.5.1. Applications for health records from solicitors or insurance companies on behalf of clients; or

5.5.2. Applications direct from patients or their relatives; and

5.5.3. Applications for access to personnel records, HR requests.

Under this legislation organisations are no longer able to charge an administration fee for completing Data Subject Access Requests.

5.5.4. As quoted within the Right of Access, ICO guidelines:

'In most cases you cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies'.

5.5.5 In such instances advice / guidance must be initially sought from the Head of Information Governance / Head of Legal Services.

6 Disproportionate Effort

6.1. The Trust should follow the guidance within the ICO SAR Code of Practice in regard to finding and retrieving relevant information, including personal data in e-mails; dealing with requests involving third party information; and the "disproportionate effort" exception.

6.2. **The "disproportionate effort" exception.**

6.3. In order to apply this exception the burden of proof is on the data controller (the Trust) to show that they have taken all reasonable steps to comply with the data subject access request and that it would be disproportionate in all the circumstances of the case to take further steps.

6.4. The issue is whether supplying the requested information would result in so much work or expense as to outweigh the requester's right to the information (the benefit to the requester of accessing the information).

6.5. You can refuse to comply with a data subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

6.6. If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

6.7. In either case you need to justify your decision and document such.

6.8. The above must be based on the request to charge a reasonable fee which reflects the administrative costs of complying with the request. If the Trust decides to charge a fee then the individual must be contacted promptly and informed. The Trust does not need to comply with the request until the fee has been received.

6.9. **E-mails**

6.10. In instances where the a data subject access request necessitates the need to review *excessive volumes* of email information the recommendation is that the Trust should carry out a *reasonable and proportionate search,* based on appropriate search criteria, to locate personal data within the e-mails.

6.11. **MS Teams**

All information captured within the MS Teams chat function is disclosable under a Data Subject Access request. Therefore, caution should be observed when using this function for communication purposes, and all users must be aware that this information is disclosable.

6.12. **Third Party Data**

6.13. As confirmed by the ICO the Trust is not obliged to supply e-mails from which another individual can be identified:

- If the other individual has not consented and
- It is not reasonable in all the circumstances to supply the information without their consent.

6.14. If the Trust is unable to obtain the consent of other individuals, the Trust must consider Steps 1 and 3 of the “Three Step Approach” set out in the ICO SAR Code of Practice

7 Exemptions

Where a senior manager determines that the records may not be disclosed or may only be partially disclosed, the reasons must be recorded. Exemptions include:

7.1 Data relating to the physical or mental health or condition of the data subject, where, in the opinion of a clinician, disclosure would be likely to cause serious harm to the physical or mental health condition of the data subject or any other persons. Guidance is available from the Head of Information Governance / Information Governance Manager or Caldicott Guardian.

7.2 The above also applies in instances where the disclosure of information contained within a HR file would be likely to cause serious harm to the physical or mental health condition of the data subject or any other persons.

7.3 Data recorded in the file supplied by a third party, who is not a health professional involved in the treatment or care given to the data subject, e.g. the data subject's family or friends, from whom no specific consent for disclosure is held.

7.2 Data processed for any crime and taxation purposes where the provision of this information would be likely to prejudice any of the crime and taxation purposes.

7.3 Data processed for the purposes of national security.

7.4 The health record of a deceased person where the patient's express wish not to disclose is recorded, or the information is not relevant to any claim arising from the patient's death.

7.4.1 In the case of a child – see section 5.4.2.

7.4.2 Where it is considered that the patient authorising access to another individual has not understood the meaning of the authorisation.

7.4.3 The Data Owner must check the ownership of the data, to ensure the data is owned by the Trust. Where doubt exists, the advice of the Head of Information Governance, Information Governance Manager, Head of Legal Services or Caldicott Guardian must be sought.

7.5 Confidential references

7.5.1 This exemption applies if you *give or receive* a confidential reference for the purposes of prospective or actual:

- education, training or employment of an individual;
- placement of an individual as a volunteer;
- appointment of an individual to office; or
- provision by an individual of any service.

7.5.2 ICO Guidance available: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed-1-0.pdf

7.6 Timetable for Access

7.6.1 A copy of the requested information must legally be provided to the applicant within *one month*.The start date is the date when a valid application is made, sufficient proof of identity and the relevant fee is received, whichever is the latest.

7.6.2 Should compliance not be possible within this period, (which should only occur in exceptional cases), the applicant must be advised in writing as soon as practicable.

7.6.3 You can extend the time to respond by a further *two months* if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

7.7 Arranging information

7.8 When gathering the information necessary to provide the data subject with all relevant information the following points must be considered:

7.8.1 Check for and remove any third party information or obtain the necessary consent. (There are exemptions to this requirement where, for example the disclosure is a health record and the third party data relates to a registered health professional; or in some cases, if it would be reasonable to include the third party information).

7.8.2 Historically staff names were redacted when completing subject access requests. This is not a standard approach as clinician information does form part of a medical record. In general terms redaction should only take place in instances where it would be detrimental to the member of staff or patient to release / receive information. This should not be a standard blanket approach.

7.8.3 It would however be 'good practice' to inform a member of staff in instances where a subject access request has been received which contained their name details

7.8.4 With health records, check with the clinician involved to decide whether disclosure would be likely to result in serious physical or mental harm to the data subject or any other person.

7.8.5 The method of delivery will be decided with the applicant, forinstance whether a meeting is to take place or whether the information is copied and posted out. The Act requires that a copy of the data be provided but this requirement may be waived where the data subject agrees; or it is not possible to supply a copy; or to do so would involve disproportionate effort.

7.8.6 Any inaccuracies in the record, corrected at the request of the applicant/data subject, shall be recorded, dated and signed. Changes must be made in agreement with the relevant manager or in the case of health records the relevant health professional / professional. If the manager or health professional does not agree with the request a note recording the matters alleged to be inaccurate must be made on the record and a copy sent to the applicant.

7.8.7 The data supplied to the applicant must be in an intelligible form.

7.8.8 The Patient Experience Team /PALS Officers/Legal Administrators/ HR SAR Administrators will check with the relevant clinician in the case of health records where an explanation of the data is necessary and offer this to the applicant.

7.8.9 This may be required for the interpretation of technical terminology or abbreviations or illegibility of the record. (If sight only of the information [rather than a copy] is requested arrangements must be made for a suitable health professional to be present to answer any possible questions as to the content of the record.

7.8.10 A non-clinician may supervise access, but cannot comment on the content of the record.

7.9 Method of Delivery

7.9.1 When the request has been processed and the information is ready to be disclosed to the applicant, a suitable method of delivery must be agreed with them.

7.9.2 Where the applicant wishes to collect health records in person, the applicant must sign to say they have received the information. If an explanation of the record is required, it must be provided by a clinician. A record of the explanation and disclosure will be made.

7.9.3 Where the information is not collected in person, a single record may be sent via the normal postal service in a double envelope. The inner envelope must be marked “Private and Confidential”.

7.9.4 Should multiple records or a tracked delivery be required, the information must be posted by ‘Special Delivery’ as opposed to ‘Recorded Delivery’, as the items will be tracked throughout the delivery process.

7.10.5 A return address must also be affixed to the correspondence should this be 'undelivered'.

7.10 History and Outcomes of the Access

7.10.1 A record of the request, its current status and completion must be recorded on the Datix or equivalent local system by the member of staff dealing with the request. A note of what information was supplied to the applicant together with any comment must be retained with the record.

7.11.2. Non-disclosure of the records

7.11.3 Where the relevant manager or a health care professional decide the data may not be disclosed, or only partially disclosed, this decision must be recorded and the reason for this provided.

7.11.4 In some circumstances it is not a requirement to inform the applicant that information has been withheld. Advice must be sought from the from the Head of Information Governance / Information Governance Manager where this action is considered appropriate.

7.11.5 The correspondence will be recorded within team specific Data Subject Access Request database(s).

8. The Right to Rectification

Thc UK GDPR includes a right for individuals to have inaccurate Personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing which must be responded to within one calendar month. However, in certain circumstances a request for rectification can be refused.

8.1 Ensuring all information recorded and held is accurate and kept up to date is essential. This is of particular importance for personal data processed by the organisation as data protection legislation places specific responsibilities on data controllers for maintaining accurate personal data.

8.2 Individuals have the right to request have inaccurate personal data rectified or completed if it is incomplete.

8.3 An individual can make a request for rectification verbally or in writing.

8.4 What actions need to be taken?

8.4.1 Any request for personal data to be rectified should be made to the organisation either verbally or in writing. Requests may be made to anyone within the organisation. Staff must ensure the details of the data subject, as well as details of any inaccuracy or incomplete

information, are recorded in writing and passed immediately to the Data Protection Officer / Head of Information Governance.

8.4.2 Whilst any request to rectify records is being assessed the processing of the personal data in question will be restricted to prevent further use and any reliance on potentially inaccurate or incomplete data.

8.4.3 If a rectification request is refused, the reason will be explained to the data subject in full and in writing within one month of the original request having been received. All data subjects who have their rectification request refused will also be informed of their legal rights to complain to the ICO and to seek a judicial remedy.

8.4.4 Where inaccurate data relating to an individual has been shared with any third-party, they should be informed of any rectification where appropriate to ensure their records can also be amended as required.

9. The Right to Erasure

9.1 Individuals have a right to request to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.

9.2 Individuals can make a request for erasure verbally or in writing.

9.3 The right is not absolute and only applies in certain circumstances.

9.4 When does the right to erasure apply?

9.4.1 Individuals have the right to request to have their personal data erased if the personal data is no longer necessary for the purpose which it was originally collected or processed for;

- Consent is the lawful basis for holding the data, and the individual withdraws their consent;
- Legitimate interest is the basis for processing, and the individual objects to theprocessing of their data, and there is no overriding legitimate interest to continue this processing;
- Personal data is being processed for direct marketing purposes and the individual objects to that processing;
- Personal data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- Erasure is required to comply with a legal obligation; or Personal data has been processed to offer information society services to a child.

Exemptions

However, there are exemptions to the Right to Erasure which does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information. To comply with a legal obligation.
- Or the performance of a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise, or defence of legal claims

9.5 Informing other organisations about the erasure of personal data

9.5.1 There are two circumstances in which other organisations need to be informed about the erasure of personal data:

- The personal data has been disclosed to others; or
- The personal data has been made public in an online environment (for example on social networks, forums or websites).

9.5.2 If personal data has been disclosed to others, each recipient must be contacted tem inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the individuals must be informed about any such recipients.

9.5.3 Recipients include natural or legal persons, public authorities, agencies or other bodie to which the personal data are disclosed. The definition includes controllers, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

9.5.4 Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

9.6 Erasing personal data from backup systems

9.6.1 If a valid erasure request is received and no exemption applies, the personal data must also be erased from backup systems as well as live systems. Individuals must be fully informed as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

9.6.2 It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

9.6.2 In circumstances where backup data cannot be immediately overwritten it must as a minimum be put 'beyond use'. Personal data which remains within any backup may no be used for any other purpose.

10 Complaints procedure

10.1 Should an individual query or disagree with any decisions made regarding a data subject access request, or should they disagree with the information provided, the case must, in the first instance, be referred to the Patient Experience and PALS Manager for review in accordance with the Trust's Complaints Policy.

10.2 The applicant may complain to the Information Commissioner. Compensation may be sought from the Trust if damage and distress has been suffered by the applicant or a third party whose information has been disclosed.

11 Responsibilities

11.1 To enable the Trust to fulfil its statutory obligations all staff must be made aware of the responsibilities they have.

11.2 **Chief Executive Officer**
The Chief Executive Officer is accountable for the administration of this policy. They have overall responsibility for the implementation of this policy. They will ensure that full commitment and support is provided and maintained in relation to the administration of this policy.

11.4 Executive Directors/ Senior Managers
Executive Directors and senior managers are managerially responsible for ensuring that this policy/procedure is implemented, communicated and monitored within their area of responsibility.

11.5 Patient Experience Lead
The Patient Experience Lead is responsible for ensuring that all SARs from patients or their relatives are managed appropriately.

11.6 Head of Information Governance
The Head of Information Governance is responsible for providing

expert advice to staff on the interpretation of the Data Protection Act 2018 / UK GDPR and related legislation; and may be involved in the resolution of complaints arising from requests for access to personal data.

11.7 Human Resource Business Partners

HR Business Partners / Advisors will be responsible for Processing requests for access to staff records.

11.8 Head of Legal Services

The Head of Legal Services is responsible for managing requests For access to health records from third parties such as the police, coroners, solicitors and insurance companies.

11.9 Operating Unit Managers (local Information Asset Administrators)

Operating Unit Managers or delegated deputy are responsible for ensuring the confidentiality and security of health records whilst on station; and for ensuring their timely delivery to the health records team.

11.10 Health Records Manager

The Health Records Manager is responsible for managing internal requests for access to health records; and where requests are judged to have a justified purpose, for delivering a copy of the health record in a timely and secure manner to the relevant staff member.

11.11 **Other Staff**

All employees must understand their duty of care to ensure the confidentiality of all personal data. In addition, they are responsible for following this policy and reporting to their manager and through the DIF - 1 process any problems relating to access to clinical or personal data.

12 Competence

12.1 All staff will receive training appropriate to their roles as identified in the Training, Education and Development Procedure.

13 Monitoring

13.1 This policy will be reviewed every two years – or sooner if new Legislation, codes of practice or national standards are introduced.

13.2 The Head of Information Governance is responsible for reviewing the policy in conjunction with the key stakeholders identified

section six of this policy and procedure.

13.3 The Head of Legal Services, Patient Experience Lead and HR Lead.

13.4 Managers are responsible for monitoring compliance with this policy and providing reports of compliance with the statutory time frame for responses to the Head of Information Governance to facilitate reports to the Information Governance Working Group on a quarterly basis.

13 Audit and Review

14.1.1 The Head of Information Governance will audit compliance with response targets through submission of quarterly reports to the Information Governance Working Group. Exceptions will be reviewed at Information Governance Working Group and feedback provided to the relevant managers.

14.1.2 All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

14.1.3 Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

14.1.4 This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

14.2 All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

15 Associated Documents

15.1 Information Governance Policy

15.2 Data Protection Policy

15.3 Records Management Policy

15.4 Complaints Policy

15.5 Freedom of Information Policy & Procedure

16 References

16.1 Data Protection Act 2018 / UK General Data Protection Regulation

16.2 Medical Records Act 1990

16.3 Access to Health Records Act 1990

16.4 Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. 2000/413)

16.5 Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (S.I. 2000/419)

16.6 Confidentiality: NHS Code of Practice, DH, 2003

16.7 NHSx Records Management Code of Practice 2021

16.8 ICO Information: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

17 Equality Analysis

17.1 The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

17.2 Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.