Essex Partnership University
NHS Foundation Trust

INDIVIDUAL RIGHTS PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG9h
VERSION NUMBER	1
KEY CHANGES FROM PREVIOUS VERSION	New procedure
AUTHOR	Legal Services Manager/Data Protection Officer
CONSULTATION GROUPS	Information Governance Steering Committee Quality Committee
IMPLEMENTATION DATE	February 2020
AMENDMENT DATE(S)	N/A
LAST REVIEW DATE	N/A
NEXT REVIEW DATE	February 2023
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	21/01/2020
RATIFICATION BY QUALITY COMMITTEE	13/02/2020
COPYRIGHT	

PROCEDURE SUMMARY

The purpose of this policy is to provide guidance to ensure all staff are aware of and comply with the Trust's statutory obligations and responsibilities in relation to the information rights held by patients, service users and staff under the Data Protection Act.

The Trust monitors the implementation of and compliance with this procedure in the following ways;

Compliance is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee.

Services	Applicable	Comments
Trustwide	✓	
Essex MH&LD		
CHS		

The Director responsible for monitoring and reviewing this procedure is Director of ITT, Business Analysis & Reporting

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INDIVIDUAL RIGHTS PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INDIVIDUAL RIGHTS PROCEDURE

Assurance Statement

The purpose of this Procedural Guideline document is to ensure that all staff understand the procedures for individuals and their representatives to exercise their individual rights under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA). This is required in order to ensure the Trust's compliance with the aforementioned legislation.

1.0 INTRODUCTION

1.1 This procedure ensures that all Trust staff are aware of and complies with the Trust's statutory obligations and responsibilities in respect of the information rights of individuals, including patients, service users and staff under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA).

1.2 This procedure sets out the processes for dealing with requests from individuals regarding the information that the Trust holds about them.

2.0 DUTIES/RESPONSIBILITIES

2.1 The accountability for the implementation and operation within the organisation of the Individual Rights Procedure and management lies with the Director of ITT Business Analysis and Reporting. The day to day responsibility for the management of the process lies with the Trust's Information Governance Team.

For the purpose of this procedure, the definition of all staff includes all personnel working for or with the Trust, or who may receive a request from an individual exercising their rights. This includes all management, permanent employees, contractors, temporary staff, bank staff, locum, consultants, and agents/agency employees (this is not an exhaustive list).

2.2 All employees of the Trust as detailed in 2.1 are required to abide by this procedure and any associated procedural guidelines. Failure to do so could place the Trust at risk of financial penalty and may result in disciplinary action.

3.0 DEFINITIONS

3.1 The Data Protection Act (DPA) 2018

The Data Protection Act works in conjunction with the GDPR regarding data processing where flexibility and derogations are permitted. It details the purpose of the UK's supervisory authority the Information Commissioners Office (ICO) and provides legislation on data processing for law enforcement purposes and intelligence services.

3.2 General Data Protection Regulation 2016 (GDPR)
The European Union (EU) legislation that became applicable in the UK on the 25th May 2018. GDPR provides protection for the rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

3.3 Processing
Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

3.4 Personal Data
Personal data is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information. This contains details that identify individuals even from one data item or a combination of data items. The following are data that are considered identifiable such as name, address, NHS Number, full postcode, date of birth, location data, such as your home address or mobile phone GPS data an online identifier, such as your IP or email address.

3.5 Special Category Data
This is personal data consisting of information as to: genetic data relating to the inherited or acquired genetic characteristics which give unique information about a person's physiology or the health of that natural person, biometric data for the purpose of uniquely identifying a natural person, including facial images and fingerprints data concerning health which reveals information about your health status, including both physical and mental health and the provision of health care services, racial or ethnic origin, political opinions religious or philosophical beliefs, trade union membership, sex life or sexual orientation (formally known as Sensitive Data).

3.6 One calendar month
A calendar month starts on the day the organisation receives the request, even if that day is a weekend or public holiday. It ends on the corresponding calendar date of the next month. For example, a request is received on 3 May. The time limit starts from the same day. The Trust has until 3 June to comply with the request**.**

Should the end date falls on a Saturday, Sunday or bank holiday, the calendar month ends on the next working day. For example, a request is received on 25 November. The time limit starts from the same day. The corresponding calendar date is 25 December, but 25 December and 26 December are bank holidays. So the organisation would therefore have until the next working day, 27 December if that was a week day.

If the corresponding calendar date does not exist because the following month has fewer days, it is the last day of the month. For example, a request is received on 31st March. The time limit starts from the same day. As there is

no equivalent date in April, the organisation has until 30th April to comply with the request.

However, if 30th April falls on a weekend, or is a public holiday, the calendar month ends the next working day.

4.0 INDIVIDUAL RIGHTS

4.1 The GDPR provides the following rights for individuals:

1. **The right to be informed**
   The Trust must be completely transparent in how we use personal data and provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with.

2. **The right of access**
   The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why the Trust is using their data, and check we are doing it lawfully.

3. **The right of rectification**
   Individuals will be entitled to have personal data rectified if it is inaccurate or incomplete.

4. **The right to erasure**
   Also known as 'the right to be forgotten', this refers to an individual's right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances.

5. **The right to restrict processing**
   Individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This can be an alternative to requesting the erasure of data.

6. **The right to data portability**
   Individuals have the right to receive personal data they have provided to the Trust in a structured, commonly used and machine readable format. It also provides the right to request that the Trust transmits this data directly to another data controller.

7. **The right to object**
   In certain circumstances, individuals are entitled to object to their personal data being used.

8. **Rights of automated decision making and profiling**
GDPR has put in place safeguards to protect individuals against the risk that a potentially damaging decision is made without human intervention.

5.0 THE RIGHT TO BE INFORMED

5.1 Information about how the Trust processes data must be clear and concise (including personal data, pseudonymised data and also anonymised data). The information must be easily accessible (for example, via a website or published on a leaflet); be written in clear and plain language (adapted if addressed to a child) and provided free of charge. This is commonly referred to as a "Privacy Notice."

5.2 What information must be provided to individuals?

The following information under GDPR is required to be provided to individuals in a Privacy Notice.

- The name and contact details of the Trust
- The contact details of the Trust's Data Protection Officer
- Purposes of the Trust's processing
- The legal/lawful basis for the processing
- Legitimate interests for processing (if applicable)
- The recipients, or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations (if applicable)
- The retention periods for personal data
- The rights of individuals in respect of the processing
- The right to withdraw consent (if applicable)
- The right to lodge a complaint with the supervisory authority (ICO)
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable)
- The details of the existence of automated decision-making, including profiling (if applicable)
- Source of the personal data (if the personal data is not obtained directly from the individual it relates to).
- Consequences for any failure to provide information to the Trust

5.3 Regular reviews should be undertaken to check the privacy notice remains accurate and up to date. If personal data is used for any new purpose(s) or the way data is being processed is changed and these are not already documented in the privacy notice it must be updated as soon as possible.

5.4 Privacy Notice information is permitted to be communicated to individuals via various media including publishing on websites / intranets / notice boards, and via leaflets / posters and communications.

5.5 The Trust has published their Privacy Notices in line with the GDPR requirements on the Trust website and intranet. The full Privacy Notices can be found at the following links:

Candidates:
https://input.eput.nhs.uk/TeamCentre/corp/legal/_layouts/15/WopiFrame.aspx?sourcedoc={D19B7C3E-D04F-4D33-A6F8-9DF5F0ED05A9}&file=EPUT%20Candidate%20Privacy%20Notice.docx&action=default&DefaultItemOpen=1

Employees:
https://input.eput.nhs.uk/TeamCentre/corp/legal/TeamDocuments/EPUT%20Employee%20Workers%20Privacy%20Notice%20Oct%202019.pdf#search=privacy%20notice

Patients/other:
https://eput.nhs.uk/privacy-policy/

6.0 THE RIGHT OF ACCESS

6.1 This right is more commonly known as 'Subject Access (SAR)'. This right gives individuals the right to request a copy of and / or to view their personal data held by the Trust. It helps individuals to understand how and why the Trust processes their data and to provide assurance that we are doing so lawfully and to ensure its accuracy.

6.2 An individual and / or their legal representative are the only people who can request access to their personal data processed by the Trust. The information detailed in the below 6.3 – 6.14 provides details of how an individual can make a request, including information about proof of identity, fees and requests on behalf of another person. Further in-depth information can be found in CPG9b Access to Health Records procedure.

6.3 The request can be made verbally or in writing to any person in the Trust and does not have to specifically state it is a 'Subject Access Request' or quote the relevant sections of GDPR or DPA as long as the individual is requesting access to personal data.

The request can be made verbally and be noted in the relevant health/staff record, details of the verbal request should then be directed to the following teams:

Clinical record requests

Access to Records

[redacted]

Corporate Records requests

Legal Team

[redacted]

Information on the Trust procedure for Subject Access Request can be found in the CPG9b Accessing Health Records Procedure.

6.4 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Access to Records and Legal Teams must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for access. If there is any concern as to the legitimacy of the request, the teams will inform the individual and ask for further clarification.

6.5 The Trust has one calendar month to respond. This is calculated from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond can be extended by a further two months if the request is complex or if a number of requests have been received from the individual. The individual must be informed within one month of receipt of their request with an explanation as to why the extension is necessary.

No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged the Trust must have recorded the reasons for charging a fee and why it is justified.

6.6 Subject Access Request (SAR) can be made via a third party. This could be a legal representative or a relative or carer. This list is not exhaustive.

If a third party makes a request the Trust need to be satisfied that the third party making the request is entitled to act on behalf of the individual. A written authority or general power of attorney should be requested.

There are no specific provisions in the GDPR but the Mental Capacity Act 2005 enables a third party to exercise subject access rights on behalf of such an individual.

Where a child is competent, they are entitled to make or consent to a SAR to access their record.

Children aged over 16 years are presumed to be competent. Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR. However, children who are aged 12 or over are generally expected to have the competence to give or withhold their consent to the

release of information from their health records. When assessing a child's competence, it is important to explain the issues in a way that is suitable for their age.

Where, in the view of the appropriate health professional, a child lacks competency to understand the nature of the SAR application, the holder of the record is entitled to refuse to comply with the SAR. Where a child is considered capable of making decisions about access to his or her medical record, the consent of the child must be sought before a parent or other third party can be given access via a SAR.

6.7 If it is decided to refuse or reject a Subject Access Request, the individual must be informed without undue delay and within one month of receipt of the request. The individual must be informed of the reason for refusal and their right to make a complaint to the ICO.

6.8 The Trust should provide means for requests to be made electronically, especially where personal data are processed by electronic means'. A Subject Access form that allows individuals to make their request via an electronic form to the Trust should they wish to is available on the Trust's website and can be emailed to the individual on request.

Although an individual may choose to use an application form, it is not compulsory under GDPR or DPA and cannot be insisted upon or used as a reason to extend or delay the one month time limit for responding.

Response to individuals must also be provided with information about how the Trust process personal data when responding to a SAR. This information is detailed in the Trust's Privacy Notice as per 5.2 and a copy of this or details of where it can be found on the Trust's website/intranet must be provided in the response to the individual.

6.9 If an individual makes a request electronically the information should be provided in a commonly used electronic format, unless the individual requests otherwise. If the individual requests that information is provided in hard copy and posted the Trust must honour this request.

Although the GDPR and DPA recommend that where possible, remote access to a secure self-service system is provided to individuals with direct access to their information. The Trust does not store records in such a way that it can provide this service.

All Subject Access Requests should be referred to the relevant Trust department immediately to be logged and dealt processed appropriately. The relevant Trust team are detailed at 6.3.

For further information regarding subject access and the procedure please refer to the CPG9b Accessing Health Records Procedure.

7.0 THE RIGHT TO RECTIFICATION

7.1 Individuals have the right to have inaccurate personal data rectified. The definition of accuracy is not provided in the GDPR; however, the DPA advises that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

This right is closely linked to accuracy principle of the GDPR. The Trust should have already undertaken measures to ensure that the personal data was accurate when obtained; however, this right imposes a specific obligation on the Trust to reconsider the accuracy when requested.

If a request for rectification is received, steps must be taken to rectify the data if deemed necessary. All arguments and evidence provided by the data subject should be taken into account and documented for audit trail purposes.

7.2 In determining whether personal data is inaccurate can be complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made should be noted in the individual's file and must not be deleted.

7.3 It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified. This is particularly the case where medical opinion is recorded.

7.4 While the case is being considered, individuals also have the right to request restriction of the processing of their personal data whilst they contest its accuracy and whilst it's being checked as detailed in 9.0 of the procedure. As a matter of good practice, processing of the data in question should be restricted whilst the data is verified whether or not the individual has exercised their right to restriction.

7.5 If the trust following review is satisfied that the personal data is accurate and does not require rectification, the individual must be informed of this and that there will be no amendment to their data. The decision for any refusal must be explained to the individual and if they are unhappy with this decision, they should be informed of their right to make a complaint to the ICO.

7.6 A request for rectification can be refused if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can either charge a reasonable fee to deal with the request or refuse it. If the Trust decides to charge a fee you should contact the individual without undue delay and within one month. The Trust does not need to comply with the request until we have received the fee.

7.7 The request can be made verbally or in writing to any part of the organisation and it does not have to mention that it is a request for rectification or refer to the GDPR. If an individual is challenging the accuracy of their data, asking for corrections, or has asked that the Trust complete data held about them that is incomplete this is a request for rectification.

Request that are made verbally by individuals can be challenging, however staff must be able to recognise that these are requests for rectification and the Trust have a legal responsibility to ensure that this is handled correctly.

Staff must ensure that they check and document the detail of any verbal request to ensure that this has been fully understood, this can help avoid later disputes about the request has been interpreted. The request should be sent to the Information Governance team ([redacted]) immediately to formally log and process.

7.8 The Trust has one calendar month from the day of receipt to respond (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond may be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

7.9 No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged the Trust must have recorded the reasons for charging a fee and why it is justified.

7.10 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Trust's Information Governance Team must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for rectification. If there is any concern as to the legitimacy of the request, the teams will inform the individual and ask for further clarification. This should not be used as a reason to extend or delay the one month time limit for responding.

7.11 The Trust will legitimately share personal data about individuals with others in the course of their duties. If personal data has been disclosed to others, the recipients must be identified and contacted and informed of the rectification or completion of the personal data, unless this proves impossible or involves disproportionate effort. The individual should have already been informed of these recipients via the Trust's Privacy Notice as detailed in 5.5.

There are some exemptions that may apply to an individual's right to rectification. This right does not apply if the use or storage of the data is necessary for:

- compliance with a legal obligation, or for performance of a task carried out the in the public interest or in the exercise of official authority
- public health reasons
- for archiving in the public interest, scientific or historical research purposes or statistical purposes and erasure would seriously impair these objectives
- for the establishment, exercise or defence of legal claims

8.0 THE RIGHT TO ERASURE

8.1 Under GDPR individuals have the right to request personal data to be erased. This is more commonly known as the 'right to be forgotten'. The right is not absolute and only applies in the following certain circumstances:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for
- The lawful basis for holding the data was consent and the individual withdraws their consent
- Legitimate interests was the basis for processing, and the individual objects to the processing of their data and there is no overriding legitimate interest to continue this processing
- The personal data is being processed for direct marketing purposes and the individual objects to that processing
- The data is being processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st Principle)
- There is a duty to comply with a legal obligation to have the data erased
- The personal data is being processed to offer information society services to a child.

The right to erasure does not apply for healthcare data processed by the Trust. Consent is not the legal basis used for processing personal data for direct care and administration in the Trust and therefore this right does not apply. The right could however apply to staff personal data and the above considerations would need to be reviewed.

8.2 A request can be made verbally or in writing to the Trust and it does not have to specifically state 'request for erasure', if a verbal request is made this can be challenging but there is a legal responsibility for Trust staff to identify that an individual has made a request for erasure. Staff must ensure that they check and document the detail of any verbal request to ensure that this has been fully understood, this can help avoid later disputes about the request has been interpreted. The request should be sent to the Information Governance team ([redacted]) immediately to formally log and process.

8.3 The Trust has one calendar month to respond from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond may be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

8.4 No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged the Trust must have recorded the reasons for charging a fee and why it is justified.

8.5 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Trust's Information Governance Team must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for rectification. If there is any concern as to the legitimacy of the request, the teams will inform the individual and ask for further clarification. This should not be used as a reason to extend or delay the one month time limit for responding.

8.6 The right to erasure also applies to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

The Trust should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet.

This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

8.7 If a request for erasure is refused the individual must be informed without undue delay and within one month of receipt of the request. You must also inform the individual of the reason for refusal and their right to make a complaint to the ICO.

8.8 There are circumstances where other organisations need to be informed about the erasure of personal data:

- Where the personal data has been disclosed to others - each recipient of the personal data must be contacted and informed of the erasure, unless this proves impossible or involves disproportionate effort.
- The personal data has been made public in an online environment (for example on social networks, forums or websites). 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.

If the request for erasure applies to special category data the right will not apply in the following circumstances:

- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices)
- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (egg a health professional).

8.9 The right to erasure 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
- For 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

9.0 THE RIGHT TO RESTRICT PROCESSING

9.1 Individuals the right to restrict the processing of their personal data in certain circumstances under GDPR. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how the data has been processed. In most cases, it will not be required to restrict an individual's personal data indefinitely, but there will need to have the restriction in place for a certain period of time.

Individuals have the right to request restriction of the processing of their personal data in the following circumstances:

The individual contests the accuracy of their personal data and you are verifying the accuracy of the data

- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;

- The Trust no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to you processing their data (the right to object), and you are considering whether your legitimate grounds override those of the individual.
- Although this is distinct from the right to rectification and the right to object, there are close links with those rights as per below:

9.2 An individual who has challenged the accuracy of their data and asked the Trust to rectify it also has the right to request the Trust restrict processing whilst we consider their rectification request; or

- If an individual exercises their right to object, they also have a right to request the Trust restrict processing while the objection is considered.

9.3 A request can be made verbally or in writing to the Trust and it does not have to specifically state 'request for erasure', if a verbal request is made this can be challenging but there is a legal responsibility for Trust staff to identify that an individual has made a request for erasure. Staff must ensure that they check and document the detail of any verbal request to ensure that this has been fully understood, this can help avoid later disputes about the request has been interpreted. The request should be sent to the Information Governance team ([redacted]) immediately to formally log and process.

9.4 The Trust has one calendar month to respond from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond may be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

9.5 No fee can be charged unless the request can be proved to be manifestly unfounded or excessive. If it is decided that it is manifestly unfounded or excessive or further copies are requested a reasonable admin fee can be charged. If challenged the Trust must have recorded the reasons for charging a fee and why it is justified.

9.6 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Trust's Information Governance Team must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for rectification. If there is any concern as to the legitimacy of the request, the teams will inform the individual and ask for further clarification. Whilst this should not be used as a reason to extend or delay the one month time limit for responding, the Trust does not need to comply with the request until we have received the additional information.

9.7 Any processing of the personal data subject to a request should be restricted whilst the accuracy or the legitimate grounds for processing the personal data is determined.

Processing includes a wide range of actions as detailed in 3.3, including collection, structuring, dissemination and erasure of data.

The Trust can undertake various methods to restrict data, including:

- Moving the data to another system temporarily;
- Ensuring the data is unavailable to users; or
- Removing published data i.e. from a website temporarily.

A note should be placed on the system that the processing of this data has been restricted.

Once the data is restricted, processing must cease except to store it and unless:

- The individual has consented;
- It is for the establishment, exercise or defence of legal claims;
- It is for the protection of the rights of another person (natural or legal); or
- It is for reasons of important public interest.

9.8 If the personal data subject to restriction has been disclosed to others, each recipient must be contacted and informed of the restriction, unless this proves impossible or involves disproportionate effort. The Trust if asked by the individual is informed of the recipients.

Ordinarily for most requests the restriction is only a temporary measure, particularly when the restriction it is on the following grounds:

- The individual has disputed the accuracy of the personal data and the Trust is investigating this; or

- The individual has objected to the Trust processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

9.9 When the Trust has made a decision on the accuracy of the personal data, or whether legitimate grounds override those of the individual, a decision can be made to lift the restriction. The Trust must inform the individual before the restriction is lifted.

As noted above, these two conditions are linked to the right to rectification and the right to object. This means that if the Trust informs an individual that the restriction is being lifted then the individual should be informed of the reasons for the refusal to act upon their rights. The individual must also be informed of their right to make a complaint to the ICO.

10.0 THE RIGHT TO DATA PORTABILITY

10.1 **I**ndividuals the right to receive personal data they have provided to the Trust in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller, the right to data portability.

The right to data portability applies when:

- The lawful basis for processing the information is consent or for the performance of a contract; and
- Processing is being carried out by automated means (i.e. excluding paper files).

10.2 This right may be exercised to include the history of website usage or search activities, traffic and location data. It does not include additional data created based on the data an individual has provided. For example, if data is provided by an individual to create a user profile then this data would not be in scope of data portability, this would be provided to an individual making a Subject Access Request.

The right only extends to personal data and not anonymous data. However, pseudonymised data that has the ability to be linked to an individual (e.g. where that individual provides the Trust with an identifier) is within scope of the right.

10.3 If the requested information includes information about others (e.g. third party data) the Trust would need to consider whether that data could adversely affect the rights of the third parties.

If the requested data has been provided by multiple data subjects all parties need to agree to the portability request. This means that agreement will have to be sought from all the parties involved.

10.4 The right to data portability entitles an individual to receive a copy of their personal data; and / or have their personal data transmitted from one controller to another controller.

Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store. This can be achieved by either:

- Directly transmitting the requested data to the individual; or
- Providing access to an automated tool that allows the individual to extract the requested data themselves.

This does not create an obligation to allow individuals more general and routine access to systems – only for the extraction of their data following a

portability request. There may be a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, both methods must be secure.

10.5 Individuals have the right to ask the Trust to send their personal data directly to another controller without hindrance, if technically feasible this should be done.

Technical feasibility of a transmission should be considered on a request by request basis by the Trust. The right to data portability does not create an obligation to adopt or maintain processing systems which are technically compatible with other organisations but to adopt a reasonable approach and not create a barrier to transmission where it is possible.

The Trust is responsible for ensuring that any transmission of data is secure and directed to the correct recipient. The Trust is not responsible for any processing undertaken by other organisations once it has provided the data.

The data can be provided to an individual, and it is possible that they will store the information in a system with less security than the Trust. The Trust should ensure that individuals are made aware of this so as they make undertake steps to ensure that they can adequately protect any data they have received.

The Trust must ensure that adequate steps have been taken to check and verify the quality and accuracy of the data.

The Open Data Handbook available at:

http://opendatahandbook.org

This explains structured, commonly used and machine readable formats further.

10.6 If the Trust receives personal data as part of a data portability request from another organisation, this must be processed in line with data protection requirements.

The Trust in deciding whether to accept and retain personal data should consider whether the data is relevant and not excessive in relation to the purposes for which it will be processed, whether the data contains any third party information and that there is an appropriate lawful basis for processing any third party data and that this processing does not adversely affect the rights of the third parties.

Should the Trust receive personal data for which there is no reason to keep, it must be deleted as soon as possible. When data is accepted and retained, it becomes the Trust's responsibility to ensure compliance with the requirements of the GDPR.

A request can be made verbally or in writing to the Trust and it does not have to specifically state 'request for data portability', if a verbal request is made

this can be challenging but there is a legal responsibility for Trust staff to identify that an individual has made a request for data portability. Staff must ensure that they check and document the detail of any verbal request to ensure that this has been fully understood, this can help avoid later disputes about the request has been interpreted. The request should be sent to the Information Governance team ([redacted]) immediately to formally log and process.

10.7 The Trust has one calendar month to respond from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond may be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

10.8 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Trust's Information Governance Team must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for rectification. If there is any concern as to the legitimacy of the request, the teams will inform the individual and ask for further clarification. Whilst this should not be used as a reason to extend or delay the one month time limit for responding, the Trust does not need to comply with the request until we have received the additional information.

10.9 You can refuse to comply with a request for data portability if it is manifestly unfounded or excessive also taking into account whether the request is repetitive in nature. If the request is refused the individual must be informed without undue delay and within one month of receipt of the request along with the reasons you are not taking action and their right to make a complaint to the ICO or the Trust can request a "reasonable fee" to deal with the request. In either case you will need to justify your decision.

11.0 THE RIGHT TO OBJECT

11.1 Individuals the right to object to the processing of their personal data. This effectively allows individuals to ask the Trust to cease processing their personal data.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes. The individual can ask the Trust to cease processing for direct marketing at any time. The Trust does not undertake direct marketing at the time of writing this policy, however the grounds for the rights have been included for the future reference of staff should it be required.

11.2 This is an absolute right and there are no exemptions or grounds for refusal. Therefore, when an objection to processing for direct marketing is received processing the individual's data for this purpose must stop.

Individuals can also object if the processing is for:

- A task that is carried out in the public interest
- The exercise of official authority vested in the Trust
- The Trust's legitimate interests (or those of a third party).

In these circumstances, the right to object is not absolute such as for scientific or historical research, or statistical purposes, and then the right to object is more limited.

11.3 The right does not necessitate an individual's personal data to be erased, and in most cases it will be sufficient to suppress their details; retaining sufficient information about them to ensure that their preference not to receive direct marketing is respected in future.

11.4 An individual must give specific reasons why they are objecting to the processing of their data when this has been processed for a task carried out in the public interest, official authority or the Trust's legitimate interests. These reasons should be based upon their particular situation. In these circumstances, this is not an absolute right and processing can continue if:

- Compelling legitimate grounds for the processing can be demonstrated, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

11.5 If deciding whether there are legitimate grounds which override the interests of an individual, the reasons why they have objected to the processing of their data should be considered.

In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (e.g. the processing is causing them financial loss); the grounds for their objection will have more weight.

In making a decision on the individual's interests, the rights and freedoms should be balanced with the Trust's own legitimate grounds. During this process, the Trust must document and demonstrate that their legitimate grounds override those of the individual.

If the Trust decide that processing the personal data does not need to stop, the individual must be informed of this decision and informed of their right to make a complaint to the ICO.

11.6 Processing for archiving / scientific / historical research / statistical purposes - Where processing personal data for these purpose, the right to object (including the right of access, rectification and restriction on processing) is more restricted and the DPA allows the UK to provide derogations from these

rights if it is likely to render impossible or seriously impair the achievement of the specific purposes.

The DPA sets out exemptions for this processing:

- Personal data is not processed by researchers to support measures or decisions with respect to particular individuals, and is not processed in such a way as will or is likely to cause substantial damage or distress to anyone.

If an objection is received, it might be possible for processing to continue if it can be demonstrated that there is legitimate reason or the processing is necessary for legal claims.

If it is decided the processing should not cease, the individual should be informed of this decision with an explanation and information relating to their right to make a complaint to the ICO.

11.7 A request can be made verbally or in writing to the Trust and it does not have to specifically state 'request for data portability', if a verbal request is made this can be challenging but there is a legal responsibility for Trust staff to identify that an individual has made a request for data portability. Staff must ensure that they check and document the detail of any verbal request to ensure that this has been fully understood, this can help avoid later disputes about the request has been interpreted. The request should be sent to the Information Governance team ([redacted]) immediately to formally log and process.

11.8 The Trust has one calendar month to respond from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

The timescale to respond may be extended by a further two months if the request is complex or a number of requests have been received from the individual. The individual must be informed within one month of receiving their request and explain why the extension is necessary.

11.9 You can refuse to comply with a request for the right to object if it is manifestly unfounded or excessive also taking into account whether the request is repetitive in nature. If the request is refused the individual must be informed without undue delay and within one month of receipt of the request along with the reasons you are not taking action and their right to make a complaint to the ICO or the Trust can request a "reasonable fee" to deal with the request. In either case you will need to justify your decision.

11.10 The Trust is not required to respond to requests, unless it is provided with sufficient details to enable the location of information, and to satisfy itself as to the identity of the individual making the request. The Trust's Information Governance Team must take every precaution that is reasonable to establish that requests are, or are not, legitimate requests for rectification. If there is any concern as to the legitimacy of the request, the teams will inform the

individual and ask for further clarification. Whilst this should not be used as a reason to extend or delay the one month time limit for responding, the Trust does not need to comply with the request until we have received the additional information.

11.11 **I**ndividuals must be informed of their right to object at the time of the first communication with them (via Privacy Notice information) where:

Personal data is processed for direct marketing purposes, or the lawful basis for processing is:

- Public task (for the performance of a task carried out in the public interest),
- Public task (for the exercise of official authority vested in the Trust), or
- Legitimate interests

If one of the above applies, the right to object should be brought, explicitly, to the individual's attention. If processing personal data for research or statistical purposes information about the right to object (along with information about the other rights of the individual) should be included in the Privacy Notice.

12.0 THE RIGHT TO PREVENT AUTOMATED DECISION MAKING

12.1 Automated decision-making and profiling is a decision made by automated means without any human involvement, an example of this is a recruitment aptitude test which uses pre-programmed criteria.

12.2 Automated individual decision-making does not have to involve profiling, although it often will do. Profiling is:

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Organisations use profiling to find something out about individuals' preferences, predict their behaviour and make decisions. Automated individual decision-making and profiling can lead to quicker and more consistent decisions, but if they are used irresponsibly there are significant risks for individuals.

12.3 GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

Automated decision-making can be carried out when this is:

- Necessary for entering into or performance of a contract between an organisation and the individual;
- Authorised by law (for example, for the purposes of fraud or tax evasion); or
- Based on the individual's explicit consent.

If processing special category personal data, the Trust can only carry out processing described in Article 22(1) if:

- There is individual's explicit consent; or
- The processing is necessary for reasons of substantial public interest

Decisions based solely on automated processing about children should not be made if this will have a legal or similarly significant effect on them.

12.4 Automated decision making including profiling is considered to be high-risk processing; therefore GDPR requires that a Data Protection Impact Assessment (DPIA) is completed. This will identify potential risks in order to have a plan in place to mitigate them.

As well as restricting the circumstances in which you can carry out solely automated individual decision-making, GDPR also:

- Requires individuals are provided with specific information about the processing;
- Are obliged to take steps to prevent errors, bias and discrimination; and
- Gives individuals rights to challenge and request a review of the decision.

For further information on DPIA's and for a copy of the proforma please refer to the Trust's CPG50e Data Privacy Impact Assessment Procedure:

12.5 The trust must ensure that we:

- Provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- Use appropriate mathematical or statistical procedures;
- Ensure that individuals can obtain human intervention / express their point of view; and obtain an explanation of the decision and challenge it;
- Put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors;

13.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

This process is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee.

14.0 POLICY REFERENCES / ASSOCIATED DOCUMENTATION

Reference should be made to the following related documents:

- Records Destruction and Retention Procedure (CPG9c)
- Data Protection Act 2018
- Information Commissioners Guidance
- Data Protection & Confidentiality Policy CP59
- Records Management Policy CP9

- Guidance for Access to Health Records Requests from DOH
- Accessing Health Records Procedure (CPG9b)

END