NHS
Yorkshire
Ambulance Service
NHS Trust

Disclosure Policy

Author: Legal Services Manager

Approved: August 2024

Document Reference	PO – Disclosure Policy – August 2027
Version	V: 2.0
Responsible Director (title)	Director of Corporate Services / Company Secretary
Document Author (title)	Legal Services Manager
Approved By	Information Governance Working Group
Date Approved	August 2024
Review Date	August 2027
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1	September 2020	Benjamin Cowell, Legal Services Manager	D	Initial draft and creation of new policy separated from Data Protection Policy and replaces Procedure for Handling Disclosure Requests under the General Data Protection Regulations 2016 and the Data Protection Act (2018).
0.2	March 2021	Benjamin Cowell, Legal Services Manager	D	Acting upon review by the Head of Legal Services.
0.3	March 2021	Benjamin Cowell, Legal Services Manager	D	Acting upon review by the Head of Risk and Assurance
0.4	April 2021	Benjamin Cowell, Legal Services Manager	D	Acting upon comments from IGWG
1.0	May 2021	Risk Team	A	Approved at TMG
1.1	February 2024	Benjamin Cowell, Legal Services Manager	D	Reviewed and updates made.
1.2	May 2024	Risk Team	D	Movie policy on to new Trust template.
1.3	June 2024	Benjamin Cowell, Legal Services Manager	D	Further review and updates made
2.0	August 2024	Risk Team	A	Policy approved within August 2024 Information Governance Working Group.
A – Approved D – Draft				
Document Author – Benjamin Cowell, Legal Services Manager				
Associated Documentation Data Protection Policy Freedom of Information Policy Courts and Evidence Policy Claims Management Policy Complaints, Concerns, Compliments and Comments Management Policy Incidents and Serious Incident Management Policy				

Staff Summary

The Data Protection Act 2018 and UK General Data Protection Regulation provides everyone with certain rights, one of which is the right of access to personal data. The Access to Health Records Act 1990 provides certain people with right of access to the health records of a deceased patient.
Yorkshire Ambulance Service NHS Trust is committed to comply with the provisions of the Data Protection Act 2018, the UK General Data Protection Regulation , and the Access to Health Records Act 1990 by providing disclosure within the statutory timescales of either a calendar / three calendar months (DPA 2018 requests) and either 21 / 40 calendar days (AHRA 1990 requests).
All requests for disclosure pursuant to the Data Protection Act 2018, UK General Data Protection Regulation and Access to Health Records Act 1990 are strictly handed by the Legal Services Department and any requests received directly by members of staff should be forwarded to the Legal Services Department without delay.
This policy does not cover disclosures under safeguarding legislation, nor does it cover disclosures made to registrant bodies – these processes are undertaken by the Safeguarding Unit and Human Resources Team, respectively.
The Data Protection Act 2018 and UK General Data Protection Regulation provide exemptions to permit disclosures to be made without the knowledge and consent of data subjects for the purposes of crime and taxation. Police forces (and other requesting authorities) are required to provide countersigned Data Protection exemption forms if data subject consent cannot / should not be obtained.
A threshold for disclosure needs to be met to warrant disclosure without the consent or knowledge of the data subject and detailed information needs to be outlined within the Data Protection exemption form provided by the police (or other requesting authority) to meet said threshold.
There are circumstances where access to data can be prevented to prevent serious harm (physical or psychological) occurring to the data subject or any other person.
Emergency out of hours disclosure should only be made when a request for disclosure cannot await being processed by the Legal Services Department during the next working day. A procedure is outlined within this policy for the Emergency Operations Centres and IUC NHS 111 call-centres.
Processes for occasions where a right to object notice or a dealing with inaccuracy notice are received by the Trust are outlined within this policy and shall require the convening of a review group to review the notice and decide as to how to proceed.
Support and guidance regarding any element of this policy can be sought from the Legal Services Department.

1.0 Introduction

1.1 The Data Protection Act 2018 and UK General Data Protection Regulation ("UK GDPR") was introduced on 25 May 2018. The Act provides data subjects (patients, staff, and others) with the following rights:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights in relation to automated decision making and profiling.

These rights are outlined in Section 3 of this policy

1.2 The Data Protection Act 2018 and UK GDPR affects data of living individuals and the right of access pertaining to data of deceased persons remains outlined within the Access to Health Records Act 1990. The Access to Health Records Act 1990 confers access to data of deceased persons to a select group of individuals, namely those who are eligible to bring a claim on behalf of the deceased's estate or a claim arising from the death of an individual. The Access to Medical Reports Act 1988 governs access to medical reports made by a patient's normal clinician for insurance or employment purposes.

1.3 All requests for disclosure of person identifiable information ("PII") are dealt with by the Legal Services Department, be it from individuals, solicitors firms, police forces or other organisations. No such information must be disclosed outside the Trust unless it has been managed and approved by the Legal Services Department in accordance with this policy and its processes. If any member of staff receives a request for access to PII, they must pass on the request to the Legal Services Department at the earliest opportunity. The only exception to this would be for statutory requests for information for safeguarding matters and information pertaining to members of staff provided to registrant bodies which will be handled by the subject matter experts in the Safeguarding Unit and Human Resources Team, respectively.

2.0 Purpose / Scope

2.1 The aim of this policy is to outline the process to be followed in response to a request for disclosure under the Data Protection Act 2018 & UK GDPR and the Access to Health Records Act 1990 which outline rights of access to PII.

2.2 This policy should be read in conjunction with the Data Protection Policy, which outlines the principles of the Data Protection Act 2018 and UK GDPR.

2.3 For processing to be lawful under the UK GDPR, the Trust must identify a lawful basis before it can process personal data. It is important that the Trust determines the lawful basis for processing personal data because this has an effect on the data subjects' rights. For instance, if the Trust relies on someone's consent to process their data, then they will generally have stronger rights to have their data deleted. Each of these rights is explained in further detail and how they impact on the Trust in the following sections.

2.4 The Trust will ensure that requests made by data subjects in relation to their rights regarding data processing are handled in accordance with the Data Protection Act 2018, UK GPDR and Information Commissioner's guidance. A process flow chart for handling a data subject's right to object under the Data Protection Act 2018 and UK GDPR, is detailed in Appendix A.

3.0 Data Subjects' Rights

The Data Protection Act 2018 and UK GDPR provide the following rights of individuals:

3.1 The Right to be Informed

3.1.1 YAS will ensure that all individuals whose details are processed by the Trust are aware of the way in which the information will be obtained, held, and disclosed. The information provided must be concise, transparent, intelligible, and easily accessible; typically, this will be done through the Trust's Privacy Policy and associated Privacy Notices which are available on the Trust website.

3.2 The Right of Access

3.2.1 Individuals also have a right to access the personal data which is held about them by the Trust. Where data is being processed by YAS and the data subject makes a request to access the data, the Trust shall provide the data subject with access to the personal data and, if requested:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed to;
- where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
- the existence of the right to request from YAS the rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data was not collected from the data subject, any available information as to their source;
- any existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- where personal data is transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

3.3 The Right to Rectification

3.3.1 Individuals also have a right for personal data to be rectified by YAS in certain circumstances if it is inaccurate or incomplete. Where a request is for the rectification of inaccurate data, the Trust shall carry this out where the request does not conflict with any legal, regulatory, or other such constraints. This may include updating personal data to include a supplementary statement. The Trust may need to inform third parties that have been sent personal data that the data subject has made a rectification request and what the rectification request was.

3.4 **The Right to Erasure (Right to be Forgotten)**

3.4.1 An individual can request the removal or deletion of their data by the Trust in certain circumstances. When requested to do so by the data subject, the Trust will erase personal data where the request does not conflict with any legal, regulatory, or other such constraints. The Trust shall inform third parties that have been sent personal data that the data subject has requested erasure (including any third parties holding data that has been made public).

3.5 **The Right to Restrict Processing**

3.5.1 Individuals also have a right to have their data suppressed by the Trust in certain circumstances. Where requested to do so by the data subject, the Trust shall restrict the use of their personal data where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the Trust to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Trust no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims; and
- where the data subject has objected to processing and the Trust are in the process of verifying whether the objection is on legitimate grounds.

3.5.2 A data subject who obtained the restriction of processing shall be informed by the Trust before the restriction of processing is lifted.

3.6 **The Right to Data Portability**

3.6.1 This allows individuals to obtain their personal data from the Trust (in some circumstances) and to reuse it for their own purposes at other organisations. The Trust shall carry out a request from a data subject to transmit personal data to another data controller without hindrance, where:

- the processing of the data is based on consent;
- the processing of the data is carried out by automated means; and
- the request does not conflict with any legal, regulatory, or other such constraints.

3.6.2 Transmitted data shall be in a structured, commonly used, and machine-readable format.

3.7 **The right to Object**

3.7.1 Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for the purposes healthcare research, including individual studies and research databases.

3.7.2 Where a data subject objects to the processing of their personal data for a specific purpose, the Trust shall no longer process the personal data for such purposes except where there are any legal, regulatory, or other such constraints.

3.8 Rights in Relation to Automated Decision Making and Profiling

3.8.1 In certain circumstances, individuals have the right not to be subject to a decision when it is based on automated processing by the Trust; and it produces a legal effect or a similarly significant effect on the individual.

3.8.2 In relation to 3.2 – 3.8, the data subject is entitled to the request being actioned free of charge, without undue delay and in any event within one month of receipt of the request (in the majority of circumstances). Therefore, if any of these requests are received by the Trust, the Legal Services Department should be contacted for advice as soon as possible.

4.0 Right of Access – General Information and Guidance

4.1 Under Section 45 of the Data Protection Act 2018 and Article 15 of the UK GDPR, subject to certain conditions and exemptions, there is an entitlement to apply for access to personal data which is sometimes known as a 'subject access request' ("SAR"). Under the Data Protection Act 2018 the request must be complied with within one month of receipt, although this time may be extended by a maximum of two calendar months for complex requests.

4.2 Most of the requests for PII made to the Trust are for health records and patient information. A health record is defined in the Data Protection Act 2018 as any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual. These records are classed under the Data Protection Act 2018 as special category data. The Data Protection Act 2018 gives rights of access to every living person, or their authorised representative, to apply for their health records irrespective of when the records were compiled. No reason is required to be provided for requesting access.

4.3 The right of access can also be for non-health related records e.g., staff personnel file, sickness file, emails etc. The Data Protection Act 2018 makes no distinction between requests made which are internal or external to an organisation.

4.4 There are exemptions within the Data Protection Act 2018 and UK GDPR which allows disclosure to be made without the explicit consent and / or knowledge of a data subject for the purposes of prevention and detection of crime and the apprehension of offenders. Please see Section 7 of this policy for more information.

4.5 All requests for such disclosures must immediately be sent to the Legal Services Department upon receipt.

4.6 The Trust has a Caldicott Guardian, whose role is to advise on the ethical as well as the legal considerations, following the Caldicott Principles. Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian. When information sharing is legally permitted, the Caldicott Guardian may need to decide how much information it is appropriate to share, in line with the third Caldicott principle. Caldicott Guardians may on occasions be asked to advise on disclosures that may be in the public interest, for example to protect individuals or society from risks of serious

harm, such as serious communicable diseases or serious crime, or to enable medical research, education or other secondary uses of information that may ultimately benefit society. Personal information may be disclosed in the public interest, without consent – and in exceptional cases where consent has been withheld – if the benefits to an individual or to society of the disclosure outweigh both the public and the patient's interest in keeping the information confidential.

5.0 Right of access – Legal Services Department procedure

5.1 The Trust's Legal Services Department responds to requests for records from patients, their personal representatives, litigation friends, lawyers, or parents. It is important to note that the right of access to personal data is that of the data subject alone. Therefore, before disclosing any records to anyone other than the patient (i.e., to a third party), the Trust must be satisfied that the patient has consented that the disclosure should be made to the third party.

5.2 On receipt of a request the Legal Services Department will request proof of identification or written consent for release and request any additional information required if these have not been provided. The Legal Services Department uses the Legal module within the DATIX record management system to process right of access requests.

5.3 Right of access requests can be made verbally or in writing and information must normally be provided free of charge. However, a charge may be made if the request is 'manifestly unfounded' or 'excessive' and there may be a reasonable charge for further copies requested.

5.4 The obligation to comply with a right of access request takes effect once the Trust has the information necessary to identify the requester and locate the information, whether this is a working day or not. The Trust has a calendar month to respond to the requester and in certain circumstances the Trust can extend this by another two months. Should a request be deemed complex, the requester should be informed as soon as possible and within a calendar month with the rationale for deeming the request as being complex.

5.5 In exceptional circumstances if it is not possible to comply within the time limit, the requester will be informed. The dates that the obligation arises and is completed are recorded on DATIX by the Legal Services Department. Key Performance Indicators for completion of the request are monitored monthly within the department.

5.6 Proof of identification is checked by having sight of photographic identification e.g., passport, driving licence and separate proof of address e.g., utility bill. Consent for release to a third party is required to be in writing and specific. These are initially requested and checked by the Legal Services Assistants.

5.7 The Legal Services Department will access the relevant databases and files to collate the data requested relating to the subject and prepare documents for disclosure. When direct access by the department is not available, the assistance from relevant persons within the Trust is relied upon to provide information, such as requests for copies of personnel files, e-mail communication etc. When documents are prepared for disclosure, it is likely to involve the redaction of third-party data (such as addresses of other individuals contained within computer aided dispatch incident logs) and this is done electronically.

5.8 The Legal Services Department will keep individual records within DATIX for each right of access request and all documentation will be scanned and uploaded to the record along with electronic copies of prepared disclosure documents.

5.9 Prior to disclosure, the disclosure bundle, consent, and proof of identification will be reviewed by the Legal Services Coordinator (FOI & Disclosure). In their absence, this can be undertaken by a fellow Legal Services Coordinator or the Legal Services Manager.

5.10 Once reviewed by the Legal Services Coordinator (or Manager), the disclosure is then sent by encrypted e-mail with a completion letter, using the NHS Mail system. This involves placing [secure] within the subject line and a user guide is sent prior to the encrypted disclosure. In certain circumstances, the disclosure may be encrypted and burnt to compact disc and then posted via recorded delivery. In exceptional circumstances, the disclosure bundle may be printed and sent via post, again by recorded delivery.

5.11 If the requestor is unhappy with the way in which his/her request has been dealt with they can contact the Legal Services Department in the first instance to be addressed by the Legal Services Coordinator (FOI & Disclosure) and with escalation to the Legal Services Manager and/or the Data Protection Officer. Should the requester wish to make a formal complaint or if the matter cannot be resolved locally within the department, the complaint shall be raised with the Patient Relations Team and processed in accordance with Section 3.16.7.3 of the Complaints, Concerns, Compliments and Comments Management Policy. Requesters are also informed of their right to contact the Information Commissioner's Office ("ICO") if they have any concerns with the way in which their request has been handled in addition to providing the details regarding their other rights as a data subject.

6.0 Right of Access Requests - Specific Circumstances and Considerations.

6.1 Access to records of children

6.1.1 A child is anyone who is under the age of 18 which is in accordance with the UN Convention on the Rights of the Child. ICO guidance states that a child may exercise their rights on their own behalf if they are competent to do so. In England, competence is 'assessed depending upon the level of understanding'. The ICO states that a child should not be deemed as competent if it is evident that he or she is acting against their own best interests. Regarding data protection legislation, a child under the age of 13 is unable to provide consent to processing.

6.1.2 If a child is not deemed to be competent, an adult with parental responsibility may exercise the right of access on the child's behalf. It is important to establish that the adult does indeed have parental responsibility – namely an adult who has the legal rights and responsibility for the child according to the law of the child's country of residence. This may not necessarily be the biological parent of the child in question and parental responsibility can be held by more than one 'natural or legal person'. A child can consent to allow the adult with parental responsibility to act on their behalf but an adult with parental responsibility cannot act without the consent of a child, if they are deemed competent.

6.1.3 Should a child be deemed as competent and by extension, presumed to be competent to exercise their own data protection rights then the right of access should be conducted directly with the child. Considerations regarding the competence of a child should also

be made and assistance should be sought from the Legal Services Coordinator (FOI & Disclosure) or Legal Services Manager if unsure.

6.2 Access to records of adults without capacity

6.2.1 For patients who because of their mental or physical condition are unable to give consent to disclosure of their health records; the decision on whether to disclose will be made in the patient's best interests by the patient's treating doctor and the Trust's Executive Medical Director. The views of families and carers will inform that decision.

6.2.2 A person appointed by the court to manage affairs on behalf of an incapacitated patient has a right under the Data Protection Act 2018 to receive information about that patient. This will be a person who holds a Lasting Power of Attorney (Health and Wellbeing) for the data subject, or a deputy appointed by the Court of Protection.

6.3 Access to records of deceased people

6.3.1 When an individual has died, information relating to that individual remains confidential under the common law[1] and the Data Protection Act 2018 and the UK GDPR cease to apply when the individual dies. It is Department of Health and Social Care and General Medical Council policy that records relating to deceased people should be treated with the same level of confidentiality, as those relating to living people. Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. Under this legislation, when a patient has died, their personal representative (executor or administrator) or any person having a claim resulting from the death has the right to apply for access to the deceased's health records. The Access to Health Records Act 1990 provides two categories of requester, namely that of the personal representative and those who may have a claim arising from the death of a person. The former category has a wider range of access (to all records) whereas the latter is only permitted access to records which relate to the intended / potential claim. These facts are verified by the Legal Services Assistants prior to disclosure and assistance sought from the Legal Services Coordinator (FOI & Disclosure) and Legal Services Manager if required

6.3.2 As the Access to Health Records Act 1990 is separate from the Data Protection Act 2018 and UK GDPR, the timescales for disclosure are different. The length of time between the record being created (or added to) and the request for access being made will determine the timescale for disclosure. If there are 40 days (or fewer) between the record being created (or added to) and the request for access, the timescale for disclosure is 21 calendar days from the date of request or receipt of all relevant information. Should there be more than 40 days between the record being created (or added to) and the request for access, the timescale for disclosure is 40 calendar days. There is no fee for making a request under this Act.

6.3.3 When the statutory medical examiner system commences on 9 September 2024, the Access to Health Records Act 1990 will give medical examiners the statutory right to access the medical records of deceased patients from the holders of those records. For the period before the statutory medical examiner system commences, following an application by NHS England and on the advice of the Confidentiality Advisory Group (CAG – an independent body which provides expert advice on the use of confidential patient information), the Secretary of State for Health and Social Care has approved the

[1] *Pauline Bluck v Information Commissioner and Epsom & St Helier University Hospitals NHS Trust* (EA/2006/0090), *Lewis v Redfern Nicholas Lewis (Claimant) v Secretary of State for Health (Defendant) & Michael Redfern QC (Interested Party)* [2008] EWHC 2196 (QB) amongst others.

use of confidential patient information for the purposes of the non-statutory medical examiner system, under section 251 of the National Health Service Act 2006 and Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 ('section 251 support'). This section 251 support is in place until 8 September 2024 and enables healthcare providers, to share the medical records of deceased patients with medical examiners. Furthermore, healthcare providers may share (and medical examiner offices may process) contact details of deceased patients' next of kin in accordance with Article 6.1(e) UK GDPR (processing that is necessary for the exercise of a public task). Medical examiner offices are based in NHS trusts/foundation trusts which process personal data in accordance with all applicable legal and NHS requirements including UK GDPR.

6.4 **Requests for Audio Recordings**

6.4.1 Audio recordings of calls are disclosed once a signed declaration limiting use of the audio recording is received by the requester. Requesters are reminded that should they wish to utilise the content of the audio recording outside of personal matters then express consent must be obtained from the Trust. Such requests would be handled by the Legal Services Coordinator (FOI & Disclosure) and the Legal Services Manager.

7.0 Police Requests - General Information and Legal Services Department Procedure

7.1 There is an exemption within the Data Protection Act 2018 to allow disclosure of personally identifiable information required for the purposes of crime and taxation (Schedule 2, Part 1, Paragraphs 2 and 3, Data Protection Act 2018).

7.2 The exemption does not cover the disclosure of all personal information in all circumstances. Information may be disclosed to the police only if it cannot be obtained from another source; if it is the minimum necessary for the stated purposes and not merely convenient, and if not releasing it would be likely to prejudice (i.e., significantly harm) any attempt by the police to prevent and investigate crime or to catch a suspect. Under these circumstances, it is not necessary to obtain the consent of the data subject. The purpose of Schedule 2 is to allow disclosure without informing the data subject or seeking consent, whereby giving that notification might prejudice the police investigation for the prevention of crime or catching a suspect. This is subject to the Department of Health and Social Care guidance detailed in Section 7.6 below.

7.3 Police requests for information must be passed to the Legal Services Department immediately via yas.policerequests@nhs.net. The Legal Services Department will process all requests whilst in hours – please see Section 8 regarding out of hours provision.

7.4 The request must be made in writing and accompanied by a countersigned Data Protection exemption form ("DPEF") by a supervising officer – preferably, an officer by the rank of Inspector or above.

7.5 If a Data Protection exemption form is not forthcoming then the Trust will not at that stage comply with the disclosure request unless the circumstances are so grave and urgent that information is required immediately without delay; an undertaking is given to provide documentation with a retrospective Data Protection exemption form. These circumstances are rare and disclosure without a Data Protection exemption form should be rare.

7.6 The Legal Services Department will determine if the exemption is appropriate in line with Department of Health and Social Care guidance regarding severity of offence and threshold for release. To justify disclosure, the circumstances of the matter must be sufficiently serious or the substantial public interest in disclosure outweighs any duty of confidence owed to the data subject.

7.7 The Legal Services Department uses the Legal module within the DATIX record management system to process police requests and the Legal Services Assistants will record the request and create a record for each request, scanning and uploading all correspondence and disclosures. The Legal Services Department will access the data requested, prepare documents for disclosure, and complete the request, noting the completion date within DATIX for key performance indicator analysis.

7.8 Prior to disclosure, the disclosure bundle, consent and/or Data Protection exemption form will be reviewed by the Legal Services Coordinator (FOI & Disclosure). In their absence, this can be undertaken by a fellow Legal Services Coordinator or the Legal Services Manager.

7.9 Once reviewed by the Legal Services Coordinator (or Manager), the disclosure is then sent by e-mail to a secure e-mail address or should this not be available via encrypted e-mail by means of the NHS Mail system. This involves placing [secure] within the subject line and a user guide is sent prior to the encrypted disclosure. In certain circumstances, the disclosure may be encrypted and burnt to compact disc and then posted via recorded delivery. In exceptional circumstances, the disclosure bundle may be printed and sent via post, again by recorded delivery.

7.10 A fee will not be charged when providing records to the police for the prevention or detection of crime, or for the apprehension or prosecution of offenders.

7.11 Court Orders received by the Trust are processed in the same manner as police requests and upon arrival, the Legal Services Coordinator (FOI & Disclosure) is notified of its existence. As with all requests, the Legal Services Coordinator (FOI & Disclosure) will review the content of the Court Order and proposed disclosure, prior to disclosure.

7.12 Requests for statements from operational personnel and the facilitation of interviews with the same must be handled by Legal Services Department staff only. Should any member of staff be contacted directly by a police officer (or other requesting authority) then the requester should be signposted to the Legal Services Department without delay. Under no circumstances should statements be provided (or interviews be undertaken) without the knowledge and direction of the Legal Services Department.

8.0 Emergency Out of Hours Disclosure

8.1 It is not the policy of the Trust to disclose personally identifiable information outside standard working hours of the Legal Services Department (Monday to Friday, 0800hrs to 1600hrs, except Bank Holidays) and any requests for disclosure received after 1600hrs will normally be processed the next working day.

8.2 Emergency requests (predominantly) from the police, may arise out of hours and in this instance the request is handled by the Emergency Operations Centres (“EOC”) in accordance with the Emergency out of hours disclosure procedure (Appendix B).

8.3 Emergency requests that are received within Integrated Urgent Care ("IUC") whilst out of hours are handled by IUC within the NHS 111 Call Centres in accordance with the Emergency out of hours disclosure procedure (Appendix B).

8.4 Emergency requests that are received within Patient Transport Services ("PTS") whilst out of hours are handled by the PTS On Call Manager in accordance with the Emergency out of hours disclosure procedure (Appendix B).

8.5 Requests should only be actioned out of hours if there is a genuine and urgent need, otherwise the request should be passed to the Legal Services Department to be processed within office hours.

9.0 Limitations Regarding Access

9.1 Under the Data Protection Act 2018 and UK GDPR, there are only two reasons why access can be denied or limited to a patient, or their authorised representative:

a) Where the data controller judges that the information disclosed may cause serious harm to the physical or mental health or condition of the patient, or any other person.

b) Where giving access would disclose information relating to or provided by a third person who had not consented to that disclosure unless it is reasonable in all the circumstances to comply with the request without the consent of the third-party individual. The Legal Services Manager will make the decision on disclosure under this exemption.

9.2 Where consent of a third party is not obtained, information should still be disclosed without revealing the identity of the third party, for example, by redaction, such that the resulting information is genuinely anonymous.

9.3 Healthcare professionals who have compiled or contributed to the health records, or who have been involved in the care of the patient, are not exempt from disclosure of third-party information about themselves.

9.4 Requests by people with parental responsibility can be denied if the child gave the information contained in their records with the express wish, or in the expectation, that it would not be disclosed to their parents.

9.5 Under the Access to Health Records Act 1990, if the deceased person had indicated that they did not wish information to be disclosed, or if the record contains information that the deceased person expected to remain confidential, then it must remain so. The same limitations on serious harm to mental or physical health and to the identification of a third person, which affect disclosure under the Data Protection Act 2018, apply equally to the records of deceased people.

10.0 Disclosure Without Consent

10.1 Occasionally it will be necessary to disclose a patient's records without their consent and, rarely, in contradiction of the patient's clear objection to disclosure. There are three possible justifications for this:

a) If it is believed that a patient may be a victim of neglect or abuse and that they lack capacity to consent to disclosure and that disclosure is in the patient's best interests.

b) If it is believed that it is in the wider public interest, or that it is necessary to protect the patient, or someone else, from the risk of death or serious harm. Examples of this might be to inform the DVLA if someone may be unfit to drive, in addition to disclosure to assist the police in preventing or solving a serious crime or informing the police if there is good reason to believe that a patient is a threat to others.

c) Disclosure is required by law for example, in accordance with a statutory obligation, or to comply with a court order or a disclosure notice from the NHS Counter Fraud Authority.

d) Requests from research studies may apply via the Health Research Authority for information – such requests are handled by YAS Research Institute and further information can be found within the Research Governance Policy.

10.2 In any of these cases, the Trust should only provide the minimum amount of information necessary to serve the purpose and the designated member of staff processing the request should carefully document the reasons for making the disclosure as approved by the Legal Services Manager or an appropriate senior manager. Advice should be sought from the Legal Services Department regarding matters pertaining to the above.

11.0 Training Expectations for Staff

11.1 Training is delivered as specified within the Trust Training Needs Analysis (“TNA”).

11.2 Staff handling right of access and police requests will receive appropriate training, development, and support to allow them to discharge their responsibilities.

12.0 Implementation Plan

12.1 The latest approved version of this policy will be posted on the Trust intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this guidance during Trust induction.

13.0 Monitoring Compliance with this Policy

13.1 The effectiveness of this policy is monitored against adherence to external timescales set by the relevant legislation. Key Performance Indicators (“KPIs”) based on the legislative timeframes have been agreed.

13.2 Compliance with timescales and KPIs are monitored by the Legal Services Manager and Head of Legal Services monthly, following reports completed by the Legal Services Administrator.

13.3 Ad hoc reports to any committees or groups shall be provided by the Legal Services Manager regarding any aspect of this policy upon request.

13.4 Information governance incidents will be monitored by both the Clinical Governance Group and the Information Governance Working Group.

14.0 References

14.1 Legislation (all available online via www.legislation.gov.uk)

- Data Protection Act 2018
- UK General Data Protection Regulation
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988

14.2 External guidance

- Information Commissioner's Office – Right of Access https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
- Information Commissioner's Office – Children and the UK GDPR https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/
- Department of Health and Social Care – Confidentiality: NHS Code of Practice – supplementary guidance: public interest disclosures https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice-supplementary-guidance-public-interest-disclosures
- Department of Health and Social Care – Confidentiality: NHS Code of Practice https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- The UK Caldicott Guardian Council – Information sharing and disclosure https://www.ukcgc.uk/information-sharing-and-disclosure
- Health Research Authority – Guidance for using patient data https://www.hra.nhs.uk/covid-19-research/guidance-using-patient-data/

14.3 Internal guidance and support

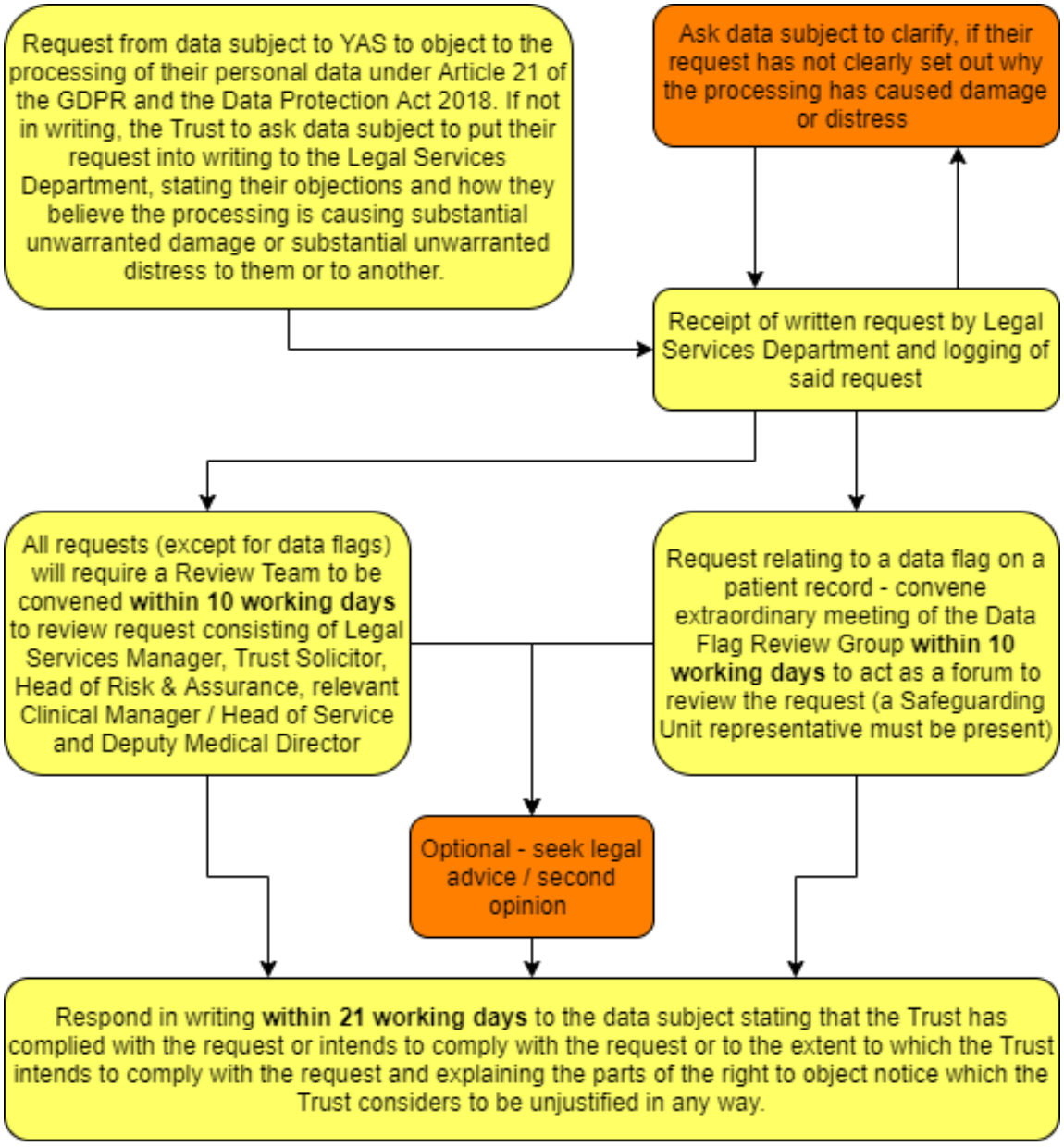
- Legal Services Department – Subject Access Requests section yas.subjectaccessrequests@nhs.net
- Legal Services Department – Police Requests section yas.policerequests@nhs.net
- YAS Publication Scheme - https://www.yas.nhs.uk/publications/publication-scheme/

15.0 Appendices

15.1 This Policy includes the following appendices:

- Appendix A – Right to object notice (Article 21 UK GDPR) process flow chart and
- Appendix B – Emergency out of hours disclosure procedure

Appendix A – Right to object notice (Article 21 UK GDPR) process flow chart



How to recognise an Article 21 GDPR notice:

1. It is important to remember an Article 21 GDPR notice may not be easily recognisable
2. It may not mention Article 21 and may form part of a lengthy piece of correspondence
3. It doesn't have to be and is most cases won't be in the form of a formal notice. For example, it could be a complainant asking for their case documents to be deleted or destroyed, albeit the regulation refers to processing, not deletion.

An individual has no right to object to processing if their personal data is required for:

1. The performance of a task in the public interest by an official authority
2. Direct marking (including profiling)
3. Historical or scientific research

Appendix B – Emergency out of hours disclosure procedure

EOC / IUC / PTS centre:		**Requesting officer:**	
Date:		**Rank:**	
Time:		**Contact telephone number:**	
Incident reference(s):		**Contact e-mail:**	
Information requested (exact):			
Reason for request:			

An emergency disclosure is one which cannot await the request being processed during office hours by the Legal Services Department

	Checklist	Yes/No	Comments
1	**Identity confirmation** Am I sure the person is who they are? Best practice to ask for name and return the call via Force Control / switchboard / office number rather than mobile and direct dial.		
2	**Emergency request** An emergency request is defined as a life-or-death situation or where immediate legal proceedings are underway. Should information not be provided almost immediately it would significantly harm the police investigation. An example of this would be a high-risk missing person or a suspect in custody.		**If the answer to this question is no, do not proceed with the request and inform the requester to send the request through to the Legal Services Department.**
3	**Data protection exemption** Confirmation that the person asking for information is doing so for the purposes of the investigation or prevention of crime and/or the apprehension of offenders. If patient consent		

	can/should be obtained, it should be obtained, and an exemption should not be relied upon.		
4	**Serious crime and impact** Confirmation that the crime is 'serious' and carries a prison sentence of more than 5 years to justify a breach of patient confidence. Does the offence involve serious physical / psychological harm to an individual and/or is there a high impact upon the victim of the crime?		
5	**Can this information be obtained by any other route?** Is it truly necessary for patient confidence to be breached, could the information be obtained from a different source?		
6	**Proportionality** Am I releasing the minimum information required to meet the purpose? If not, reduce for an affirmative response.		

Information disclosed:			
Disclosed by:		**Position:**	
Data Protection exemption form received?	Yes / No	**If not, is it be followed?**	
Copy of this form and DPEF sent to the Legal Services Department (yas.policerequests@nhs.net)			