East of England Ambulance Service NHS Trust

Data Protection Policy

Document Reference:	POL022
Document Status:	Approved
Version:	V12.0

DOCUMENT CHANGE HISTORY

Initiated by	**Date**	**Author (s)**
Information Governance Group		Helen Edmondson
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
V2.0	September 2009	Approved at Trust Board
V3.0	19 November 2013	Recommended at IGG
V4.0	28 November 2013	Approved at ELT
V4.0	23 February 2015	Review date extension agreed by IGG following approval by EMB
V5.0	17 December 2015	Approved by Executive Leadership Board
V6.0	May 2018	Reviewed by IG team
V6.1	January 2019	Reviewed by IG team
V6.1	March 2019	Approved by IGG

V7.0	20 March 2019	Approved by Management Assurance Group
V7.1	July 2019	Approved IGG Chair's Action
V8.0	30 July 2019	Approved by Management Assurance Group
V8.1	May 2020	Reviewed by IG Team
V8.1	19 May 2020	Recommended at IGG
V9.0	18 June 2020	Approved by Compliance and Risk Group
V9.1	February 2022	Review by IG Team and DPO
V9.1	May 2022	Recommended at IGG
V10.0	June 2022	Approved by CRG
V10.1	February 2024	Review by IG Team and DPO
V10.1	May 2024	Recommended at IGG
V11.0	June 2024	Approved by CRG
V11.1	April 2026	Review by SAR Manager and IG Manager
V12.0	June 2026	Approved by Risk and Policy Group

Directorate:	Digital
Recommended at Date	Information Governance Group 18/05/2026
Approved at Date	Risk and Policy Group June 2026
Valid Until Date	June 2029
Equality Analysis	Completed May 2026
Linked procedural documents	Records Management Policy Information Governance Policy Freedom of Information Policy Management of Incidents Policy Patient Care Record Policy Disciplinary Policy
Dissemination requirements	To be sent to all staff working with release of information
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage / civil partnership, pregnancy / maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

1.0 Introduction

Everyone working in the NHS has the responsibility to collate, store and process data in a secure way in line with the Data Protection Act 2018, UK General Data Protection Regulations (UK GDPR), Access to Health Records Act 1990 and current guidance from the Department of Health, Information Commissioner's Office and other regulatory organisations.

The Information Commissioner was set up in 2001 as an independent authority to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner governs the release of information from NHS Trusts and we are ultimately responsible to the Information Commissioner for any information breach or incidents.

2.0 Purpose

This document sets out the Trust's responsibilities to individuals in relation to data protection, including the release of information procedure for the East of England Ambulance Service NHS Trust ("the Trust"). The legal framework governing the use of personal confidential data in health care is complex. It includes the NHS Act 2006, the Health and Social Care Act 2012, the Data Protection Act 2018, the UK GDPR, Access to Medical Reports Act 1988, Access to Health Records Act 1990 and the Human Rights Act 1998.
It aims to provide guidance and a structured approach to processing and releasing information both internally and externally.

3.0 Types of requests for information

Requests for information take a variety of forms. Most requests for non-person-identifiable information, corporate information or information not related to a specific incident do not fall under this policy and should be dealt with under the Freedom of Information policy. If a request is received and it is unclear which policy to use, contact should be made with your line manager or advice sought from the Information Governance Manager.
Requests for person-identifiable data (PID) from patients or their representatives are known as subject access requests (SAR) and

should be processed in accordance with the current data protection legislation and this procedure. If the patient is deceased, the request should be processed under the Access to Health Records Act 1990 and in line with the Common Law Duty of Confidentiality.

Requests for person-identifiable data from the Police, Coroner, GP, NMC (Nursing and Midwifery Council), GMC (General Medical Council), HCPC (Healthcare Professions Council) and Counter Fraud Authority should also be dealt with under this policy as well as requests from staff.

Examples of the information that can be requested are the Patient Care Record, ePCR, Computer Aided Dispatch, call recordings, body worn camera footage. personnel file, Occupational Health records, earnings information, emails and/or call recordings. This list is not exhaustive.

3.1 Air ambulance/private ambulance service or third-party records relating to Trust business

Requests for records/documents should be processed by the Information Governance Department in line with the normal procedure. However, requests for interviews or the completion of statements/questionnaires should be dealt with by the air ambulance or private ambulance service. The Information Governance Department should receive a copy of the statement/questionnaire/interview notes for Trust records.

4.0 General Data Protection Regulation and Data Protection Act 2018

As of 25 May 2018 the main pieces of legislation governing data protection are the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Under this legislation there are seven principles to govern how person-identifiable data is processed:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.

5. Storage limitation (For only as long as it is needed).
6. Integrity and confidentiality (security).
7. Accountability.

The legislation introduces increased rights for data subjects, including the following:

- the right to be informed about the collection and the use of their personal data (this information is contained within the Trust's Privacy Notice on the website)
- the right to access personal data and supplementary information (see section 4.1 below)
- the right to rectification, have inaccurate personal data rectified, or completed if it is incomplete
- the right to erasure (to be forgotten) in certain circumstances (excluding health records or public health/scientific research purposes)
- the right to restrict processing in certain circumstances
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services
- the right to object to processing in certain circumstances (direct marketing, legitimate interests or performance of a public task, scientific/historical research/statistical purposes)
- rights in relation to automated decision making and profiling (the Trust does not perform these operations)
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner

In relation to all of the aforementioned data subject rights, these will be logged by the IG team on the Trusts request management system. Advice will be sought from the Trust's Data Protection Officer (DPO) and relevant departments / subject matter experts where required.

The Trust is required to respond to the requester within one calendar month.

4.1 Subject Access Requests

Under the Data Protection Act and UKGDPR, an individual or their representative (e.g. solicitor) is entitled to ask an organisation if they hold information on the individual and, if so, they are entitled to a copy of that information. These requests are known as subject access requests.

An individual can make a SAR verbally or in writing. It can also be made to any part of EEAST (including by social media) and does not have to be directed to a specific person or contact point.

The Trust must comply with this request within one calendar month of receiving the request or on receipt of any further information that the Trust has requested from the individual in order to locate the information. All requests will be logged onto the Trust's request management system.

In line with the Data (Use and Access) Act, where a data subject request or data access request is unclear or incomplete, the organisation may formally pause ("stop the clock") the statutory response timeframe while seeking reasonable clarification from the individual, with the time limit resuming once sufficient clarification is received.

The current process to be followed when releasing information will depend on who has requested it ("the Applicant"). As most requests are processed electronically, it is important that the SARs team are assured that they are corresponding with the correct individual and they will complete extensive checks to ensure this is the case. The matter will be referred to the Data Protection Officer if there are any concerns about the identification of the requester and the DPO may undertake additional checks.

- **Individual/patient**

The GDPR does not set out formal requirements for a valid request. Therefore, an individual can make a SAR verbally or in writing. It can also be made to any part of your organisation (including by social media) and does not have to be directed to a specific person or contact point. In addition, proof of identity and address will be obtained before we send out any information e.g. copy of passport and utility bill.

- **Third party**

Third parties requesting information about individuals must have the patient's consent before the information is released. If a third party contacts the Trust requesting information, the Information Governance Department will write to the patient with a consent form asking the patient to sign and return the consent form allowing the Applicant to act/request information on their behalf.

- **Solicitors**

Solicitors or their agents often act on behalf of patients or members of the public in order to submit subject access requests. Providing that a valid form of authority has been signed by the patient, the Information Governance Department should treat the solicitors as representatives of the patient and release the information requested to them. It is important to ensure that the form of authority covers all of the information requested by the solicitors e.g. the patient may agree to the Patient Care Record being released to the solicitors in relation to a particular incident however they may not have agreed for all records we hold on them to be released to the solicitors.

There may be occasions when the patient does not have capacity to consent to the release of information and a relative/solicitor is requesting this on their behalf. In these situations, the IG Department should ask to see a copy of the Court of Protection/Deputy order or a Power of Attorney. These are all legal documents that show the person has been appointed to act on the patient's behalf. The Trust appreciates that this document may not always be available however it will release information providing the Applicant is the next of kin and has proof of their identity. These types of requests should be referred to and approved by the Information Governance Manager.

4.2 Requests from the Police

Requests for information from the police should also be dealt with under the current data protection legislation but these do not constitute subject access requests. The release of data will fall under the DPA 2018 Schedule 2, Part 1, Paragraph 2 and GDPR Article 6(1)(d). In order to use this exemption, the Applicant will make the request in writing via the Data Protection Act(DPA) Form

(signed) and specify which subsection they are requesting the information under. The DPA form must be signed by the Police Officer requesting the data, and counter-signed by a higher ranking officer approving the request. The IG Department will review the request and ensure that the Applicant has provided enough information to show the exemption is being used correctly. If not, they are entitled to contact the Applicant and request further information. Once the IG Department are confident that the reason provided is legitimate, they will release the information requested to the Applicant.

The police may require information urgently out of normal office hours, e.g. suspect in custody, in these situations the police may contact the Emergency Operations Centre and present the DPA form electronically to the Duty EOC Officer. The Duty EOC Officer will perform the checks outlined above, ensuring the form is appropriately signed, and release the information to the police officer if appropriate. The Duty EOC Officer will be responsible for sending all information (including the completed Data Protection form and their response) to the IG Department by emailing SARS@eastamb.nhs.uk.

5.0 Preparing and releasing the information

EEAST will conduct reasonable and proportionate searches to locate personal data, and is not required to carry out excessive, speculative or unreasonable searches, consistent with the Data Protection Act 2018 and provisions under the Data (Use and Access) Act.

The Information Governance Department will ensure that any third-party information is redacted before sending out records as this should not be released without the third party's consent. This includes call recordings, CCTV or any other visual recordings.

The information should be checked for clarity, and any business or medical terms should be explained.

Any information in relation to a third person is removed unless:

- The third party is a professional who has compiled or contributed to the record or who has been involved in the care of the patient.
- The third party, who is not a health professional, gives their consent to the disclosure of that information.
- All reasonable steps have been taken to contact the third party without success, and ensuring any duty of confidentiality owed to that person.

Any information likely to cause serious harm to the physical or mental health of the data subject or any third person if it were to be released be removed.

Information sent out consisting of personal data should only be released in the following ways:

- By email through designated secure work email account or via standard email providing the documents are encrypted.
- If the person wishes to collect the information from a locality office then this should be signed for and identification shown.
- Via Royal Mail special delivery (proof of delivery). All letters to be headed as Private and Confidential.

All documents must be marked as "Requestor's Copy" in one of the following ways prior to release.

- All electronic copies of documents must be watermarked as "Requestor's Copy" on each page. They must include the relevant reference number, the name of the recipient and the date of the release. These documents must then be converted and saved into a format which prevents alteration, such as encrypted PDF, prior to sending.

All electronic documents will be sanitised, encrypted and password protected before being released to the Applicant.

Person-identifiable information should never be released over the telephone.

On occasions the Trust will receive requests for statements/interviews with a member of staff. Initially the Applicant should be asked to send in a list of questions for the member of staff. If the Applicant is reluctant to do this or this has already been completed and an interview is required, the interview should be arranged through the locality management team and the Applicant should be charged in accordance with the fees agreed by the Data Protection Officer. Staff details should never be provided externally without their prior consent.

6.0 Coroner Requests

Requests for information from the Coroner do not fall under the data protection legislation. These requests must still be in writing however the Trust has an ongoing positive duty to the Coroner to disclose information relevant to the death (Coroner's Justice Act). All Coroner requests are managed by the Legal Services Department via a Coroners e-mail address coroners@eastamb.nhs.uk so that all requests made can be logged and managed as a matter of urgency as time is of the essence to obtain the necessary written evidence and to arrange for staff to attend the inquest. These requests must be dealt with within 4 weeks. The Legal Services Team has produced specific guidance around Coroner's requests and inquests, which is available on the Trust's intranet.

7.0 Internal Requests

It is common for managers to require person-identifiable information as part of an investigation for a complaint/claim/incident. This should be released providing that the request has been made in writing (an email is sufficient) and that a reason has been provided for this, e.g. to investigate a Datix incident. These requests should be dealt with by the relevant department (e.g. Patient Safety Department to process requests for records relating to patient safety incidents; Patient Experience Department to process requests for records relating to complaints; Information Governance Department to process requests for Information governance breaches).

7.1 CCTV / Vehicle CCTV / Body Worn Camera footage

Requests for CCTV, Vehicle CCTV and/or body worn camera footage are to be sent to the Subject Access Request team via SARS@eastamb.nhs.uk. A proforma will be required to be completed by the requesting manager. Reasons for requesting the footage will be reviewed by the Information Governance Department and, if approved, the team will request footage ready for release, including undertaking any redaction required. If the release is refused, full reasons will be provided to the manager. Further information on Audio Visual systems can be found in the Audio-Visual Systems Policy Framework.

7.2 Estates ID Card audits

Requests for Estates ID Card audits are to be sent to the Subject Access Request team via SARS@eastamb.nhs.uk. A proforma will be required to be completed by the requesting manager. Reasons for requesting the audits will be reviewed by the Information Governance Department, if approved the team will request the information from the Estates Team to release. If the release is refused, full reasons will be provided to the manager.

8.0 Safeguarding Requests

Requests for information contained within the Patient Care Records and Computer Aided Dispatch (CAD) records in relation to any safeguarding referrals made by the Trust where no consent is required, will be dealt with by the Safeguarding Team.
The Safeguarding team will release this information in line with the UKGDPR and Data Protection Act 2018.

Any other requests relating to Safeguarding will be logged and processed by the IG Department in line with this policy.

9.0 Requests from existing or former employees for personnel files

Subject Access Requests from existing or ex-employees are allocated to the Subject Access Request team situated within the Information Governance Department.

The Subject Access Request team has an approved process for dealing with requests. An individual can make a SAR verbally or in writing. It can also be made to any part of EEAST (including by social media) and does not have to be directed to a specific person or contact point.

If a request is received from an employee via the individuals Trust email account, this is considered to be sufficient identification for the individual and further ID is not required. For requests not received via a Trust email account, ID must be provided and verified prior to releasing the information.

These requests will be logged on to the Trust's SAR management system. The Trust has one calendar month to comply with the request, if the request is considered as complex the Trust may extend this the time to respond by a further by two months. The Trust must let the individual know and explain why the extension is required.

All medically related requests, i.e. requests for occupational health records, will be dealt with by the Trust's Occupational Health team.

If the SAR relates to a disciplinary, which is being managed under the Trust's Disciplinary Policy, and requires aspects of the request related to the disciplinary process to ensure proceedings can continue, the SARs team will prioritise this part of the request. The employee is required to indicate to the SARs team what parts of the SAR are required to progress their case. All aspects of the SAR will still be completed; however the disciplinary-related parts will be prioritised to assist the timeliness of the disciplinary process.

10.0 Requests from other regulators

The Trust receive requests from regulators, including The Health and Professionals Council (HCPC), Nursing and Midwifery Council (NMC) and Counter Fraud. These requests require a Pro-Forma to be completed before the Trust releases documents to these regulators. These types of requests are managed by the Subject Access Request Team via the SARS e-mail address SARS@eastamb.nhs.uk so that all requests made can be logged and handled correctly.

11.0 Access to Health Records Act 1990

Requests for information relating to an individual who has died should be dealt with in line with the Access to Health Records Act 1990. Although there are no specific timescales afforded by the Act it is likely that organisations will be expected to respond within one calendar month. Technically the only two groups of people who are allowed access to the patient's health records are:

- the personal representatives or
- Anyone with a claim arising out of the patient's death.

In order to show that the Applicant has been appointed as the personal representative the IG Department will ask for a copy of the Grant of Representation (formerly known as Grant of Probate or Letters of Administration). The Trust understands that these documents are not always available so will accept requests from the next of kin providing they have proof of identity and taking into account the patient's wishes before they died. These requests will need to be approved by the Information Governance Manager if the team are unsure. The Information Governance Department will also consider the confidentiality principles when releasing this information.

12.0 Caldicott Guardian principles and purpose

Every NHS Trust must appoint a Caldicott Guardian. The Caldicott Guardian manual identifies eight principles that should always be taken into consideration when releasing any person-identifiable information. These are:

- Principle 1: Justify the purpose(s)
- Principle 2: Don't use patient-identifiable information unless it is absolutely necessary
- Principle 3: Use the minimum necessary patient-identifiable information
- Principle 4: Access to patient-identifiable information should be on a strict need to know basis
- Principle 5: Everyone should be aware of their responsibilities
- Principle 6: Understand and comply with the law

- Principle 7: The Duty to share information can be as important as the duty to protect patient confidentiality.
- Principle 8: Inform patients and service users about how their confidential information is used.

The Caldicott Guardian can be contacted if you have any queries in relation to data protection or releasing information via the Information Governance Manager.

13.0 Complaints and claims

If the Applicant is unhappy with the release of information process in any way, then the Applicant should contact the Information Governance Department in order to resolve this. If the Information Governance Department cannot resolve this informally then the Applicant should raise their complaint formally with the Trust's Data Protection Officer, DPO@eastamb.nhs.uk. The DPO will review the complaint and provide an independent assessment of the request and response provided by the SAR team.

The Applicant also has the right to complain to the Information Commissioner: www.ico.org.uk.

Any claims in relation to the Trust's data protection activities will be managed by the Legal Services Team.

14.0 Record Keeping

All requests for information will be logged and managed on the Trust's request management system; no paper files will be kept. Access to the release of information files will be confined to the Information Governance Department and for audit purposes when all person-identifiable information will be removed. The records will be stored and disposed of in line with the Trust's Records Management policy and retention/disposal schedule.

The Safeguarding and Legal Services team maintain their own release of information files and access is confined to members of the relevant team.

15.0 Incidents

Any incident involving a potential breach of the Data Protection Act 2018 or the Access to Health Records Act 1990 should be reported as an incident using the DATIX reporting system. A decision will be taken whether it is necessary to report this as to the Information Commissioner by the Information Governance team using the NHS England Data Security and Protection Toolkit incident reporting tool to support this decision.

16.0 Monitoring

Compliance with the Data Protection 2018 and UKGDPR will be monitored by the Information Governance Manager and Data Protection Officer. Reports on requests relating to data subject rights received IG Department will be sent to the Information Governance Group on a bi-monthly basis where the volume and compliance will be discussed and reviewed, with any escalations sent to the Compliance and Risk Group. Any recommendations by the Information Governance Group will be actioned with oversight from the Trust's Caldicott Guardian and SIRO and lessons will be shared and disseminated by the IG Department.

Appendices

A Monitoring Table
B Equality Analysis

Appendix A - Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
DPA 18 and GDPR Compliance	Information Governance Manager and the Data Protection officer	Progress reports from the SAR team. Compliance reports	Bi-monthly updates at IGG Annual report to Board	Compliance reports and written report where needed	Review by Information Governance Group and Compliance and Risk Group. Compliance reports will be discussed Any decisions will be recorded in the minutes of the meeting	Information Governance Manager with support from the IG and SAR teams	Review of SAR process, to improve the overall compliance and have more responses sent to the data subject on time.

Appendix B

Equality Impact Assessment

EIA Cover Sheet

Name of process/policy	Data Protection Policy
Is the process new or existing? If existing, state policy reference number	POL022
Person responsible for process/policy	IG Manager
Directorate and department/section	Governance
Name of assessment lead or EIA assessment team members	Information Governance Manager
Has consultation taken place? Was consultation internal or external? (please state below):	Internal: Information Governance Group
The assessment is being made on:	Written policy involving staff and patients Training programme

Equality Analysis

What is the aim of the policy/procedure/practice/event?
To ensure that the Trust and its staff protect the information that it holds and complies with all current UK Data Protection Legislation. This includes the processing of personal identifiable data, its storage, use and retention. Further to this it also covers the processing of special category data such as those items listed below. This policy protects the rights of all those groups mentioned below.

Who does the policy/procedure/practice/event impact on?

Age X
Disability X
Gender X
Gender re-assignment X
Marriage/Civil Partnership X
Pregnancy/maternity X
Race X
Religion/belief X
Sexual orientation X

Who is responsible for monitoring the policy/procedure/practice/event?

The Data Protection Officer, The Senior Information Risk Owner and the members of the Information Governance Group (IGG)

What information is currently available on the impact of this policy/procedure/practice/event?

This policy and the Laws that underpin it are directly designed to impact all Data Subjects and ensure that their data is respected and protected.

Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? No

Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No, If yes please provide evidence/examples:

Age X
Disability X
Gender X
Gender re-assignment X
Marriage/Civil Partnership X
Pregnancy/maternity X
Race X
Religion/belief X
Sexual orientation X

Please provide evidence:

Please can I refer you to https://ico.org.uk/action-weve-taken/
This site gives practical examples of how the legislation is having a positive effect on data protection covering all groups including those with protected characteristics. This Policy is already covering all of our services users and staff in the same positive way and therefore those with protected characteristics.

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? Yes/No, if so please provide evidence/examples:
Age , Disability , Gender, Gender re-assignment , Marriage/Civil Partnership, Pregnancy/maternity , Race, Religion/belief, Sexual orientation.

Please provide evidence: No

Action Plan/Plans - SMART
Specific
Measurable
Achievable
Relevant
Time Limited

Evaluation Monitoring Plan/how will this be monitored?

Who: Information Governance Manager
How: Escalation of issues
By: SAR Team and other managers
Reported to: Information Governance Group, DPO and SIRO