East of England Ambulance Service NHS Trust

Data Protection Policy

Document Reference	POL022
Document Status	Approved
Version:	V7.0

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 Information Governance Group
V7.0	March 2019	Approved by Management Assurance Group

Author: Emma Sears (Information Governance Manager)	
Document Reference	Relevant Trust objective: Records Management Directorate: Clinical Quality
Recommended at Date	Information Governance Group 12th March 2019
Approved at Date	Management Assurance Group 20 March 2019
Review date of approved document	2 years from approved date
Equality Analysis	
Linked procedural documents	Records Management Policy Information Governance Policy Freedom of Information Policy Management of Incidents Policy Management of Serious Incidents Policy Patient Care Record Policy
Dissemination requirements	To be sent to all staff working with release of information
Part of Trust's publication scheme	Yes / No?

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, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Paragraph		Page
1.0	Introduction	4
2.0	Purpose	4
3.0	Types of requests for information	4
4.0	General Data Protection Regulation and Data Protection Act 2018	5
5.0	Preparing and releasing the information	7
6.0	Coroner requests	8
7.0	Internal requests	9
8.0	Safeguarding requests	9
9.0	Requests from existing or former employees for personnel files	9
10.0	Access to Health Records Act 1990	9
11.0	Caldicott Guardian principles and purpose	10
12.0	Complaints	10
13.0	Record-keeping	11
14.0	Incidents	11

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 current data protection legislation, 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 General Data Protection Regulations (GDPR), Access to Medical Reports Act 1988, Access to Health Records Act 1990 and the Human Rights Act.

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 information from patients or their representatives are known as subject access requests 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 information from the Police, Coroner, GP, NMC (Nursing Medical Council), GMC (General Medical Council) and HCPC (Healthcare Professions Council) 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, Adastra (out of hour's records), personnel file, Occupational Health records, earnings information 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 and they should charge the applicant directly for this information. 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

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

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.

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 5.1 below)
- the right to 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 DATIX and referred to the Data Protection Officer who will respond in person or via the IG team following consideration of the application, with the exception of the right to access, which will be managed in line with the process below.

4.1 Subject access requests

Under the current data protection legislation, 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.

The Trust has to comply with this request within thirty calendar days 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 on DATIX.

The current process to be followed when releasing information will depend on who has requested it ("the Applicant"). The Information Governance Department will also send out an Equality and Diversity Form in relation to the Applicant for those requests made by individuals:

- **Individual/patient**

Requests by members of the public or staff for information we hold on them must be in writing and signed. In addition proof of identity and address must be obtained before we send out any information e.g. copy of passport and/or utility bill.

- **Third party**

Third parties requesting information about individuals are usually relatives however we must always have patient consent before releasing any information. If a relative 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. It is likely that these requests will colloquially be known as s.29 requests or DPA requests (as under the DPA 1998 the Trust could choose to release information to the police due to a discretionary exemption contained within s.29 (the Crime and Taxation exemption)). The new exemption is contained within the DPA 2018 Schedule 2, Part 1, Paragraph 2. In order to use this exemption the Applicant will need to make the request in writing and specify which subsection they are requesting the information under. 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.
On occasion the police will require information urgently e.g. suspect in custody. The police may contact the Emergency Operations Centre in these situations and present the Data Protection Form electronically to Duty EOC Officer. The Duty EOC Officer will perform the checks outlined above and release the information to the police officer if appropriate. The Duty EOC Officer will be responsible for sending all information (including their response) to the IG Department by emailing eoeasnt.rfl@nhs.net.

5.0 Preparing and releasing the information

The Information Governance or Human Resources 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 fax to a safe haven (not preferred)
- 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. All letters to be headed as Private and Confidential.

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 Coroner has an absolute right to all information including personal data and medical information/records of an individual. This is due to historical case law and the Civil Procedure Rules 1998. The Coroner requires the information to conduct Inquests which are legal inquiries into the cause and circumstances of a death and is limited, fact finding inquiries. A Coroner will consider both written and oral evidence during the course of an inquest. The Coroners duty to hold an inquest is contained in section 6 of the Coroners and Justice Act 2009. Inquests are public hearings and can be held with or without juries - both are considered equally valid. Under Rule 8 of the Coroners (Inquest) Rules 2013, Coroners are required to complete an inquest within 6 months of the date on which the Coroner is made aware of the death, or as soon as is reasonably practicable. Therefore all Coroner requests are managed by the Information Governance Department via a Coroners e-mail address eoeasnt.coroners@nhs.net 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.

Coroners have the power to call witnesses to appear at an inquest, and to determine the evidence to be heard. It is the general duty of every citizen (under common law) to attend an inquest if they are in possession of any information or evidence that details how a person came to their death. Notification to appear as a witness will generally be informal, but a Coroner can issue a summons where a witness absents themselves without explanation. Summonses are issued under the Coroner's common law powers and are governed by the directions set out in the Civil Procedure Rules. Non-attendance can result in being held in contempt of court or receiving a fine.

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. These requests should be dealt with by the relevant department (e.g. Patient Safety Department to process requests for records relating to incidents or serious incidents; Patient Experience Department to process requests for records relating to complaints; Information Governance Department to process requests for claims).

8.0 Safeguarding requests

Requests for information contained within the Patient Care Records and Computer Aided Dispatch records in relation to any safeguarding referrals made by the Trust where no consent is required, will be dealt with by the Safeguarding Team and logged on DATIX.
The Safeguarding team will release this information in line with the Information Sharing: Guidance for Practitioners and Managers (see reference below) produced by the Department of Education. This enables the Safeguarding team to release information without consent for three main purposes:

- Release of the information is in the public interest
- For the safety and wellbeing of an individual
- Others who may be affected by the person's actions

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 appropriate locality HR team. On occasion it may be necessary to assign the request outside of the locality.

The Human Resources department has an approved process for dealing with requests. All requests must be made in writing or via email (preferably from the individual's Trust account). 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 DATIX.

All medically related requests will be dealt with by People Asset Management (PAM), the Trust's Occupational Health provider.

10.0 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 thirty days. 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 IG Manager if the team are unsure. The IG Department will also consider the confidentiality principles when releasing this information.

11.0 Caldicott Guardian principles and purpose

Every NHS Trust must appoint a Caldicott Guardian and the Medical Director has been appointed as the Caldicott Guardian for the Trust. The Caldicott Guardian manual identifies seven 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.

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

12.0 Complaints

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 Local Authority and NHS Complaints Regulations 2009 by contacting the Patient Experience Department or alternatively by contacting the Trust's Data Protection Officer. More information on making a complaint can be found in the Trust's Complaints policy or on our website.
The Applicant also has the right to complain to the Information Commissioner: www.ico.org.uk.

13.0 Record keeping

All requests for information will be logged and managed on DATIX; no paper files will be kept. Access to the Release of Information files will be confined to the IG Department (or HR team for staff subject access requests) and for audit purposes, when all person-identifiable information will be removed.
The Safeguarding team maintain their own Release of Information files and access is confined to members of the Safeguarding team.
The records will be stored and disposed of in line with the Trust's Records Management policy and retention/disposal schedule.

14.0 Incidents

Any incident involving a potential breach of the current data protection legislation 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 a Serious Incident under the Serious Incident Policy and/or to the Information Commissioner by the Information Governance team using the NHS Digital Data Security Protection Toolkit incident reporting tool to support this decision.

15.0 Monitoring

Compliance with the Data Protection 2018 and GDPR will be monitored by the Information Governance Manager and Data Protection Officer. Reports on requests relating to data subject rights received by the HR Department, Safeguarding Department and 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. 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.