London Ambulance Service NHS Trust

Data Protection Subject Access Request Procedure

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To provide the framework for the handling and processing of SARS correctly, and in a timely manner, throughout the Trust.

.

Sponsor Department: Corporate Governance

Author/Reviewer: Data Protection Officer. To be reviewed by May 2019.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
21/05/18	0.2	IG Manager	Procedure draft
18/05/18	0.1	Head of Workforce Analytics	People & Culture process draft

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
ELT	25/05/18	1.0
Ratified by (If appropriate):		

Published on:	**Date**	**By**	**Dept**
The Pulse	25/05/18	Internal Comms team	Comms
LAS Website	25/05/18	Internal Comms team	Comms
Announced on:	**Date**	**By**	**Dept**
The RIB	05/06/18	IG Manager	IG

Equality Analysis completed on	**By**
22/05/18	IG Manager
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
TP012	Data Protection Policy	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

Data Protection legislation gives a data subject (patient/staff) the right to obtain confirmation that their data is being processed, and where that is the case, access to the personal data.
The right of access to this information is referred to as Subject Access Request (SAR). This procedure explains the process to ensure SARs are handles line with the legislation.

2. Scope

This procedure covers all SARS received from the public, staff and ex-staff for access to their personal data and which are responded to by Patient Experiences, People & Culture, and IM&T.

3. Objective

To ensure that the correct actions take place to fulfil SAR requests in a timely manner within the Data Protection Policy framework

4. Responsibilities

4.1 The **Trust Board** is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives. The Trust as a body corporate is a data controller.

4.2 The **Chief Executive** has overall responsibility for ensuring that compliance with Data Protection legislation is managed responsibly within the Trust.

4.3 The **Director of Corporate Governance** has strategic responsibility for Information Governance including compliance with the Data Protection Act throughout the Trust.

4.4 The **Caldicott Guardian** is responsible for protecting the confidentiality of patient and service-user information and this procedure supports the Caldicott function.

4.5 The **Chief Information Officer** is the Senior Information Risk Owner (SIRO) and has strategic responsibility for the management for information risk.

4.6 The **Data Protection Officer** is responsible for providing specialist data protection advice and guidance and for developing specific guidance notes on data protection issues. The DPO is responsible for ensuring that SARS are handled within the framework of the legislation.

4.7 The **Information Governance Manager** is responsible for providing day to day advice on Information Governance matters including Data Protection issues.

4.8 **IM&T Infrastructure Management** are responsible for the provision of emails within the timeframe required to satisfy SAR requests from People & Culture.

4.9 The **Head of Patient Experiences** is responsible for the handling and processing of Subject Access Requests by the Patient Experiences Department made under the legislation.

4.10 The **Head of Workforce Analytics** is responsible for coordinating the handling of Subject Access Requests received from staff and ex-staff.

4.11 The **Information Governance Group** (IGG), chaired by the Chief Information Officer who is the Senior Information Risk Owner (SIRO) and the Director of Corporate Governance, will monitor the implementation of this procedure.

4.12 The **Executive Leadership Team** and **Heads of departments** are responsible for ensuring that the policy is implemented in their directorates and individual departments.

5. Definition

5.1 **Right of access by the data subject**

A data subject is entitled to obtain from the Data controller:

- confirmation as to whether or not personal data concerning him or her
- is being processed, and
- where that is the case, access to the personal data and the information covered in the legislation.

6. Who can make a request?

Persons who are entitled to access personal data under this procedure are:

a. The data subject.

b. A representative of the data subject who has written consent (e.g. solicitor; a court appointed representative if the subject could no longer manage his or her own affairs; a person with enduring power of attorney or quite simply anyone else an individual wants acting for them).

c. The parent or guardian of a child under 16 years of age: In cases where the child agrees, or it was in the child's best interest for access to the data to be granted.

7. What is a valid subject access request?

The LAS is not obliged to comply with a Subject Access Request unless it has received:

a. A request in writing.

b. Enough information to identify the data subject.

c. Enough information to identify the information sought.

Any request from a personal representative of the data subject should be accompanied by an authority from the data subject consenting to that individual or organisation acting on their behalf.

A subject access request may apply to any personal data held by the Trust. If the information does not fulfil the definition of personal data then the Trust does not have to disclose it in response to a subject access request (although it may choose to do so at its discretion).

A request can be very broad such as, 'give me a copy of all the information you hold about me', or it can be very precise, such as 'give me a copy of the letter you wrote about me yesterday'.

It is unlikely that the first contact from the data subject will provide all the relevant information, in which case the Trust will write to the data subject. [The model letters in Appendix 2 may be used, depending on how much further information is required].

The Trust has 30 calendar days (including weekends and holidays) to provide the information requested once it has received the necessary information.

8. Understanding the types of requests

There are two types of request that the Trust is likely receive:-

a. Routine informal requests for information which may be managed without recourse to the General Data Protection Regulation 2016, for example, "can I have a copy of my course certificate".

b. Formal requests for access to information under GDPR. e.g. "can I have a copy of my medical record" or "please provide all information held about me by the People & Culture Department". This is a formal Subject Access Request.

9. What to do with a subject access request

9.1 Request received from member of the public/patient or solicitor

When a SAR is received by Patient Experiences (PED) from a member of the public/patient or solicitor pn behalf of a client it will be logged on to Datix and confirmation of receipt will be sent to the applicant. Any request received elsewhere in the Trust from a member of the public, patient or solicitor should be forwarded to PED without delay. PED will follow their internal process for handling and responding to these requests.

9.2 Request received from member of staff or ex-member of staff

When a SAR is received from a member of staff or ex-member of staff it should be forwarded to the Head of Workforce Analytics (HWA) who is responsible for co-ordinating the response for all employment related subject access requests.

9.2.1 Verifying the data subject's identity

Before disclosing any personal information the Trust will verify the identity of the data subject. The Act requires the Trust to take 'reasonable measures' to verify the identity of a data subject. The Trust will verify their identity from their circumstances, such as their address or signature and if further verification is required then the following will be considered:

- By phone

The individual will be telephoned and asked two questions based on the information held about them to confirm their identity.

- In writing

The individual will be written to and asked to send a photocopy of their passport or drivers licence as proof of identity (this option will take longer and it is also possible that the individual does not have a passport or drivers licence).

9.2.2 Once received, the HWA will assign the request to the relevant People & Culture Manager and the timescales will be agreed. The P&C Manager will be responsible for requesting and obtaining the relevant records which may include training records (via the Education Team), the personal files (held by People & Culture Manager and line manager) and the recruitment record (via Head of Recruitment).

9.2.3 Where emails have been requested, then the HWA will co-ordinate this with the IM&T team. IM&T will conduct a search within a one week period and make available electronically the relevant emails. These emails will then need to be reviewed by the People and Culture Manager and any redactions made before they are issued as required by the data subject.

Once all the information has been collected it will be checked and examined in detail by the People and Culture Manager to establish if it should be disclosed. Final approval for disclosure will be provided by the HWA. There is guidance in Appendix 1 to support this part of the process.

9.2.4 Keeping a record

A file will be created by the HWA for each subject access request to include:

- Copies of the correspondence between the Trust and the data subject, and internally between staff in relation to the SAR process

- A record of any telephone conversation used to verify the identity of the data subject.

- A record of any decisions and how the Trust came to those decisions.
- Copies of the information sent to the data subject. This information will be kept for three years (except where there has been an appeal where the information will be kept for six years) and then securely destroyed.

9.2.5 Logging the request

The request will be logged by the HWA using the request monitoring template. This is used to track and monitor the number of information requests received and the costs incurred.

10. Repeat requests

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Trust may:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request.

Advice should be sought from the DPO or the Information Governance Manager before responding to the individual.

11. Appeals and complaints process

Data subjects have the right to appeal against a decision to refuse access to their information. If the data subject wishes to complain, this should be referred to the DPO or the Information Governance Manager. The data subject should be given the opportunity to either write their letter of complaint or express their complaint orally with a possible satisfactory outcome.

Data subjects are also free to contact the Information Commissioner, who is ` the compliance lead on Data Protection:

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Tel: 0303 123 1113 (local rate) or 01625 545 74 (national rate)

web: https://www.ico.gov.uk

The individual raising a complaint about the way their subject access request has been dealt with should be encouraged to raise the matter with the Trust before raising the matter with the Information Commissioner.

IMPLEMENTATION PLAN	
Intended Audience	All LAS staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.
Communications	New policy to be announced in the RIB and a link provided to the document.
Training	DP training is provided to new staff at Corporate Induction and to existing staff by annual online IG training. DP SAR training to be provide to staff who handle SARS as required.

Monitoring:

Aspect to be monitored	**Frequency of monitoring AND Tool used**	**Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported**	**Committee/ group responsible for monitoring outcomes/ recommendations**	**How learning will take place**
Number of SARS received and responded to on time	Quarterly	DPO IGG	RCAG	Review of process and provide training as required
Number of referrals to ICO	Quarterly	DPO IGG	RCAG	Review of process and provide training as required

Appendix 1

Guidance on reviewing data

How to blank out exempt and/or irrelevant information

When answering a subject access request you may have to blank out parts of a document which are not liable for disclosure.

Hard copy documents

- Print out the document or, if it is a paper record, make a photocopy.
- Using a black marker pen, blank out the exempt information.
- Make a photocopy of the blanked out version. This is the copy that will go to the person making the request.

Electronic documents

- Using the highlighter tool, highlight the exempt information in black.
- Save the blanked out version as a separate copy.

Check the data subject

Check that the record is actually about the person concerned and not about someone else with the same name. For example, an email might carry the subject line 'Meeting about Tom Smith' but if the email only contains details about whether people can attend the meeting, the email is not about Tom Smith.

You should only print out documents or emails which are about the person making the subject access request.

Screen out duplicate records

For example, if you have had an email exchange with some colleagues you only need to print out the last email in the exchange if previous correspondence is included within it.

Remove data about other individuals

You should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of

individuals, including the data subject, you should not disclose the information about the third parties.

- If the record is primarily about the data subject, with incidental information about others, you should blank out the third party information (see above).

- If the record is primarily about third parties, withhold it if blanking out is not possible.

- Contact the third party to obtain consent to disclose the document if possible.

The records may contain correspondence and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity, and Trust staff.
In these cases we are required to balance the interests of the third party against the interests of the data subject and often blank out third party information. If this situation arises, please contact the records management section for further guidance.

Confidential references

Do not disclose confidential references written by members of staff to bodies other than the Trust. However, we do have to disclose references received by the Trust.

For example, if you give a reference for one of your staff, you do not have to disclose that reference in response to a subject access request. However, if you have received a reference for one of your staff, that reference does not qualify for an automatic exemption.

Preventing and detecting crime

Do not disclose information which would prejudice the prevention or detection of a crime.
For example, if the police informed us that the data subject is under investigation, but the data subject did not know this, then that information should not be provided to the data subject whilst the investigation is in progress.

However, if the investigation is closed or if the data subject has been informed that there is an investigation underway, then the information should be disclosed.

Legal advice

Do not disclose any records which:

- contain advice from our lawyers
- contain requests for legal advice

- were written as part of obtaining legal advice

Negotiations

Do not disclose information which is being used, or may be used in future, in negotiations with the data subject, if the information gives away our negotiating position and disclosing the information would weaken our negotiating position.

Unfavourable information

You may discover material which does not reflect favourably on us. For example, you may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed.

However, you should bring their contents to the attention of the HWA or relevant manager, and ensure that appropriate action is taken to address any issues they raise.

You must not destroy or refuse to disclose records because they would be embarrassing to disclose: this is a criminal offence if it is done after you know a subject access request has been made.

Letter Templates **Appendix 2**

Letter Confirming Receipt Template

Letter Confirming the Identity of the Requester Template

Letter for Further Information Template

Letter Confirming Consent of the Data Subject Template

Subject Access Response Letter Template