Derby & Derbyshire LMC
Local Medical Committee

01332 913800
ddlmc.office@nhs.net
www.derbyshirelmc.org.uk

DDLMC & DDLMC LTD Subject Access Request Policy

Introduction

This policy outlines the procedures for managing Subject Access Requests (SARs) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It ensures that DDLMC responds to requests for personal data in a lawful, transparent, and timely manner.

Scope

This policy applies to:

1. All DDLMC staff, contractors, and volunteers.
2. All personal data held by DDLMC in any format (electronic, paper, audio, etc.).
3. Requests made by data subjects or their authorised representatives.

Definitions

Subject Access Request (SAR): A request made by an individual to access their personal data.

Data Subject: The individual to whom the personal data relates.

Data Controller: The organisation that determines the purpose and means of processing personal data.

Personal Data: Any information relating to an identified or identifiable individual.

Legal Framework

1. UK General Data Protection Regulation (UK GDPR)
2. Data Protection Act 2018
3. Access to Health Records Act 1990 (for deceased individuals)
4. ICO Guidance on SARs

How to make an SAR

SARs can be made:

1. In writing (email or letter)
2. Verbally (in person or by phone)

Requests should ideally be directed to the LMC's Chief Executive or Practice Liaison Officers, but any staff member receiving a SAR must forward it immediately to one of the above mentioned staff.

Verification of Identity

Before processing a SAR, the LMC must verify the identity of the requester. Two forms of ID are required, and they should be,

1. Photographic ID such as a passport or driving licence.
2. Separate proof of address such as a utility bill or bank statement (dated within the last 3 months)

3. However, if there is evidence that DDLMC has previously corresponded with the individual making the request and the contact details are unchanged and previously verified then DDLMC is able to exercise discretion when requesting proof of identity.

Responding to an SAR

DDLMC are required to provide a full response promptly, but in any event within 'one calendar month' of receipt of a valid request. The deadline should be calculated from the day a request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last

day of the following month. If the corresponding calendar date in the next month fall on a non-working day (weekend or bank holiday), the date of disclosure will fall on the next working day.

The timeframe begins after the individual has complied with the validity requirements, such as provision of satisfactory ID.

DDLMC may extend the timeframe for responding by a further two months where requests are complex or numerous. If this is the case, the individual must be informed of this within one month of the receipt of the request and be informed why the extension is necessary.

Information will be provided in a concise, intelligible, and accessible format, preferably electronically.

SARs are free of charge unless the request is manifestly unfounded or excessive.

Exemptions

The LMC may withhold information if:

- It includes personal data of another individual, unless consent is obtained, or it is possible to remove (redact) the third party's information/identity or any information which would identify them.
- It is legally privileged. This means information that is protected from disclosure in legal proceedings because it involves confidential communications between a client and their legal adviser made for the purpose of obtaining legal advice.
- It would cause serious harm to the physical or mental health of the data subject or another person.

Third Party Requests

Requests made on behalf of a data subject (e.g., by a solicitor or relative) must include written authorisation from the data subject as well as fulfilling the full verification of identity requirements.

Steps to Take When a Request is Received

1. If a request is made verbally (via telephone or in person), the member of staff who receives the request must treat it as a formal SAR and alert the CEO or PLO team the same day.

2. If a SAR is received by email, it must be forwarded the same day.
3. If a SAR is a hard copy letter it must be date stamped, then scanned and sent the same day to the CEO or PLO team.

On receipt of a SAR, the CEO or PLO must

1. Check whether the request meets the Validity Requirements. If not, missing information must be requested.
2. Send the individual an acknowledgment response within 5 working days from the date on which the request was received.
3. CEO/PLO should check the reporting systems to assess whether any personal information about the requester has been processed.
4. The CEO/PLO should review all the available information in preparation for disclosure. If the data subject's information is linked to third party information, consider the Third Party Information Steps.
5. The response must be sent within the Timeframe for Responding.
6. The response must be securely packaged, particularly for addresses abroad. Emails must be sent via NHS secure email encryption facility. Envelopes and packages must always be marked 'Private and Confidential' and 'addressee only'. A postal method where the delivery of the response is 'recorded' should be used such as Royal Mail Signed For.
7. A full copy of the original, disclosed, and withheld information must be kept on the SAR file for future reference. SAR files must be destroyed 2 years after the date of last correspondence.

Record Keeping

A log of all SARs will be maintained, including:

1. Date received.
2. Identity verification
3. Date of response
4. Summary of data disclosed or reason for refusal.

The SAR log is stored on SharePoint.

Complaints

If a data subject is dissatisfied with the response to their SAR, they may:

1. Contact the LMC's Directors for a review.
2. Lodge a complaint with the Information Commissioner's Office (ICO).

Policy Review

This policy will be reviewed every two years or sooner if there are significant changes in legislation or guidance.

Version Number	Reviewed & Ratified By	Date	Next Review date
V1	Tim Skinner	07.10.2025	07.10.2027
V2 – No changes made	Hayley Scott	18.06.2026	18.06.2027