GENERAL DATA PROTECTION REGULATION 2016

(GDPR)

&

DATA PROTECTION ACT 2018

FAQs

LMC LAW LIMITED

8 PETERBOROUGH ROAD, HARROW, HA1 2BQ

Company Registered in England in Wales

Registration Number 08977566

Subject Access Requests (SARs)

1) Q: A Solicitor has made a SAR for a patient's notes electronically, can I insist that the patient comes to collect the record from the Surgery to give to the Solicitor?

A: No, you cannot insist, you may suggest kindly and carefully that picking it up may be a good idea for reasons of security, but the law says that you need to provide the record in the manner in which is it asked.

Article 15(3) states that '…Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form'.

2) Q: If a patient has no objection to collecting the notes to pass on to the Solicitor and the Solicitor objects and wants the notes sent directly to him, what is the position?

A: The patient's wishes are paramount. The patient is the subject. If the patient wants to collect the notes, then record the consent and his wish to do so and the date it was given.

3) Q: If a Solicitor asks for the whole medical record and will not give a specific issue/time period for which he needs the notes, can this be counted as excessive and can we charge a fee?

A: No. You cannot charge a fee unless you feel the request is 'manifestly unfounded or excessive'. There is no clear definition of this so any challenge on this ground will have to be reasonable.

4) *Q: Where we have a request for patient information from the Department For Work and Pensions (DWP) in respect of a Universal Credit application do we need to check with the patient that they have given their consent?*

A: In this situation, you can supply information to the DWP without obtaining consent. The DWP have a legal basis for asking for this information under Section 8 of Data Protection Act 2018 and Article 6(1)e of the GDPR and with regard to sensitive information, section 10 of the Data Protection Act 2018 and Article 9(2)b of the GDPR.

CCTV

1) Q: Do we have to include references to external CCTV in our Privacy Notice or do we leave it out?

A: You need to include a reference to the CCTV if it is your camera. If the CCTV is located in a car park and the CCTV belongs to you then this will still be the case whether the car park is yours or not.

If the camera belongs to the car park owners, it is their responsibility and this is usually the case whether the car park belongs to them not you.

The issue centres on whether you are holding and controlling the footage. If you do hold the footage then that means you are subject to the GDPR and the Data Protection Act 2018 rules around SARs requests.

Breaches

1) Q: What is regarded as a breach and what should be reported?

A: The Data Security and Protection Toolkit is an online self-assessment tool that you must use if you have access to NHS patient data and systems. This will help you assess whether an incident should be reported. There is guidance to help you assess whether an incident should be reported at (https://www.dsptoolkit.nhs.uk/Help/29)

Once you notify the incident it will be managed by the Information Commissioner's Office (ICO) using their case management system.

Summary Care Record (SCR)

1) Q: Do we need express consent from all our existing patients when we share summary care records with other health professionals?

A: Consent is not the legal basis for processing information collected in the SCR. The legal basis for collecting information for the SCR is legal obligation and the management of health and social care systems. Authorised healthcare professionals such as emergency doctors, community pharmacists and other care staff that are involved in the patient's direct care have access to it.

Patients can ask to view or add information to their SCR such as long-term health conditions and significant medical history. The record is created automatically and the patient has a right to opt out.

Texting

1) Q: Are we able to text patients their information such as results of a blood test?

A: You should always be careful when texting information about patient health care and should have systems in place to ensure:

- *you are texting the correct person*
- *the number you are texting is correct*
- *the information you are texting is accurate*

If you choose to use this method you should make it clear that you do so in your Privacy Notice. You should also make it clear on posters or communications in your Surgery that you use texting as a method of sending test results and that patients should always ensure they inform the Surgery of any changes to their contact details.

Data Protection Officer (DPO)

1) Q: How do we decide which issues a DPO should deal with and which responsibilities fall to our Practice?

A: The Practice and the DPO should work together and document clearly their respective responsibilities. The Practice will have to ensure that the DPO is adequately assisted and resourced.

If you use an external DPO, then make sure you have a clear contract in place to establish:

a) What the DPO will do for the Practice; and,

b) The extent of the external DPO's responsibility.

External DPO's, for example, are unlikely to deal with your SARs requests so you will need to make this clear both in the contract and in your Privacy Notice to ensure that SARs requests are directed promptly to the right person.

Redaction

1) Q: What information should be redacted when sending out a SAR?

A: Information that identifies a third party where that third party has not given their consent. This is because the third party also has a right to have his 'rights and freedoms' protected.

Information relating to a healthcare worker or professional caring for a patient may be disclosed.

The ICO guidance on this states that 'The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- *the other individual has consented to the disclosure; or,*
- *it is reasonable to comply with the request without that individual's consent.*

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- *the type of information that you would disclose;*
- *any duty of confidentiality you owe to the other individual;*
- *any steps you have taken to seek consent from the other individual;*
- *whether the other individual is capable of giving consent; and,*
- *any express refusal of consent by the other individual.*

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.'

Separated Parents

1) Q: Does the Practice have to inform the other parent in the situation where the parents are separated and one parent requests access to their child's medical record?

A: No, there is no obligation on the Practice to inform the other parent although there may be circumstances (where it is in the child's best interest) where the Practice should consider doing so. This should be decided on a case by case basis.

Data Protection Impact Assessment (DPIA)

1) Q: Does a DPIA need to be completed for services currently provided or is this is for new projects or major changes in the current service provision?

A: A DPIA may be used for new commissioned services such as extended hours hubs where the processing is '*likely to result in a high risk to the rights and freedoms of individuals'. It should be used for services provided outside core contract work.*

However, our interpretation is that it is likely you will, in time, have to go back and complete a DPIA for current commissioned services.

Preparing a DPIA is something your Data Protection Officer should be able to help you with.

Notes

These FAQs are based on our interpretation of the legislation and the guidance provided by the ICO on their website. How you provide information and comply with GDPR should be done in line with the ICO's advice.

Further FAQs are provided by the Information Commissioner's Office (ICO), Information Governance Alliance (IGA) and British Medical Association (BMA) and we would refer you to their websites for further guidance.

These FAQs are updated frequently.

Version 1 October 2018