GENERAL DATA PROTECTION REGULATION 2016 (GDPR)

An Overview

Shanee Baker - Director/Lawyer, LMC Law

LMC LAW

WHAT IS GDPR?

- Part of a wider package of reform in respect of data protection: new Data Protection Act, new IG Toolkit, new national data opt-out developed by NHS Digital.

- Effective 25th May 2018
- Applies (where GPs are concerned) mainly to personal and sensitive data they hold on patients: **no real change**
- BUT… it imposes a few more obligations on GPs and healthcare organisations where compliance is concerned
- The Regulations define "**special category**" data which will need more safeguarding because it is more sensitive - GPs will be subject to more stringent rules because of healthcare data they hold

LMC LAW

CURRENT OBLIGATIONS

Don't panic – you have time to show compliance, this is an ongoing process and it won't end on 25th May:

- If you handle patient sensitive information you will have to protect that
- Only collect for a specific purpose
- Keep it secure
- Ensure it is relevant and updated
- Only hold as much as you need

GPs AS DATA CONTROLLERS

What is a Data Controller?

- Person or organisation determining ***"the purposes and means of the processing of personal data"*** - GPs are Data Controllers of patient information
- A Data Processor ***"processes personal data on behalf of the data controller"*** – GPs can also be Data Processors
- The legal responsibility is on the Data Controller to ensure that any processing of the data they collect by any third parties is **controlled and compliant**
- There should be a contract in place between the Data Controller and Data Processor

LMC LAW

GPs AS DATA CONTROLLERS continued

- Obligation of the GP Data Controller is to ensure access to data is **secured** and only accessed by staff providing **direct care** to an individual patient - to meet this obligation Practices must ensure, for example: confidentiality clauses are written into staff contracts

- Ultimately as Data Controllers, GP Practices have responsibility for handling all requests for access to data and even if they delegate responsibility **they are still responsible**.

- NOTE: GPs need to establish both a **lawful basis** and a **special category condition** to process special category data.

LMC LAW

LAWFUL BASIS FOR PROCESSING

Need to identify the **lawful basis** for processing. This can include:

- **Consent - article 6.1(a):**
  - *You need to have clear consent, not implied – so patients have to tick a box if that's how you are obtaining consent*
  - *If verbal, then note it*
  - *Think about your registration of new patients*
  - *You need separate consent for different things*
  - *Tell patients how to withdraw consent*
  - *Record consent properly*
  - *Review consent regularly*

- **Contract – article 6.1(b):**
  - *The processing is necessary for a contract you have with the individual*

LMC LAW

LAWFUL BASIS FOR PROCESSING continued

- **Legal Obligation – article 6.1(c):**
  - *The processing is necessary to comply with a legal obligation*

- **Vital Interests – article 6.1(d):**
  - *The processing is necessary to protect someone's life*

- **Public Task – article 6.1(e):**
  - *The processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. NOTE: this is the likely lawful basis that GPs will use to process: NHSE powers to commission health services under the NHS Act 2006 together with powers to delegate to CCGs*

LMC LAW

ESTABLISHING A SPECIAL CATEGORY CONDITION

GPs will also have to establish a "**Special Category Condition**" for processing as follows under Article 9:

9.2(a) *– the data subject has given explicit consent to the processing of those personal data for one or more specified purposes…*

9.2(b) *– processing is necessary for the purposes of carrying out the obligation and exercising specific rights of the controller or of the data subject in the field of employment and social security…*

9.2(c) *– processing is necessary to protect the vital interests of the data subject or any other natural person where the data subject is physically or legally of incapable of giving consent.*

LMC LAW

ESTABLISHING A SPECIAL CATEGORY CONDITION continued

9.2(d) *– processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not for profit body with a political, philosophical religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contract with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject.*

9.2(e) *– processing relates to personal data which are manifestly made public by the data subject*

LMC LAW

ESTABLISHING A SPECIAL CATEGORY CONDITION continued

9.2(f) *– processing is necessary for the establishment, exercise or defence of legal claim or wherever courts are acting in their judicial capacity*

9.2(g) *– processing is necessary for reasons of substantial public interest on the basis of union or member state law which shall be proportionate to the aim pursued…*

9.2(h) *– processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health or social care systems and services on the basis of union or member states law or pursuant to contract with a health professional and subject to the condition and safeguards referred to in paragraph 3 (common law duty of confidentiality)*

LMC LAW

ESTABLISHING A SPECIAL CATEGORY CONDITION continued

9.2(i) *– processing is necessary for the reason of public interest in the area of public health…*

9.2(j) *– processing is necessary for archiving purposes in the public interest, scientific or historical research purposes…*

LMC LAW

DATA PROTECTION OFFICER (DPO)

- GPs may be classed as public authorities under the GDPR (similar to FOIA)
- If so, then highly likely you will need a DPO (a named person) – you may have someone already (Caldicott Guardian)
- Especially if you carry out large scale processing of special category data
- DPO will need to be trained, can be an employee, cannot be conflicted – this essentially means cannot determine purpose, use, or management (governance role)
- May not therefore be a Partner
- Can act for several practices
- If a federation then DPO reports to Board

DATA PROTECTION OFFICER (DPO) continued

- A DPO is protected – can't remove them if they report you to the ICO
- Particular skill set: requires knowledge of the GDPR and other legislation around data protection
- Needs to understand the practice and the information that the practice handles
- Needs to be aware of data security
- Needs to conduct audits and monitor compliance

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

- Also known as PIAs
- Probably the duty of the DPO
- You will need to carry out this assessment when you are processing large scale special category data **where this is likely to result in high risk to rights and freedoms of individuals** e.g. extended hours hubs, clinical pharmacist agreements, mergers/super-partnerships and provision of other commissioned services
- This is to assist organisations in identifying their DP obligations and meet the requirements of privacy for the patient
- See ICO code of practice for conducting PIAs

LMC LAW

PRIVACY NOTICE

- Sometimes referred to as “Fair Processing Notices” - Very important to get this right
- It needs to be simple, clear and easy to understand
- It needs to state:
  - *Contact details of Practice as the data controller*
  - *Contact details of DPO*
  - *What personal information you hold (usually patient medical data)*
  - *Purpose of holding it (could be for a variety of reasons but essentially for medical care)* - ***need to state here the legal basis and special category condition***
  - ***Other legal bases if processing is for reasons other than direct care***

cont…

LMC LAW

PRIVACY NOTICE continued

- *What you plan to do with it and how you use it*
- *Whether you are collecting for others (e.g. the commissioner)*
- *Whether there are other data controllers and processors*
- *Whether you are creating new personal information (all the time)*
- *Retention period*
- *Right to make a complaint to ICO*

- You can't charge for it!

LMC LAW

PRIVACY NOTICE continued

- You may need a separate one for children and they need it **simplified** says the ICO

- Don't forget your **employees**: they may need a separate one. e.g. workflow minimum data set as well as holding personal information on them

- The employee privacy policy should be relatively straightforward

LMC LAW

A FEW MORE RULES

- Patients have rights of access - but the GP may redact the file online by coding as you enter information on third parties
- Can't provide access unless you have removed references to third parties
- Beware letters and documents that are scanned onto the record before GP has sight
- Patients can request amendment, correction, erasure – but no absolute right to be forgotten
- Right of erasure does not apply to a persons health record or care record or for public health or scientific research purposes

LMC LAW

SUBJECT ACCESS REQUESTS (SAR)

- SAR – time to comply shortened to a month (was 40 days before)
- Can extend to 2 months if complex, or numerous requests
- No fee – but can charge if unfounded, excessive, or repetitive
- Fee based on admin costs
- Nasty solicitor requests: manage these carefully!
- Beware CQC inspections re compliance

BREACH/PENALTIES

- Notify the ICO within 72 hours if you are aware of any breach
- Notify serious breaches without delay!
- Notify the individual directly

- Fine between 2% of annual turnover or 10 million Euros (whichever is higher)
- For really serious breaches 4% of annual turnover or 20 million Euros (whichever is higher)
- Can also include warnings, bans on processing
- Fines and penalties meant to be **proportionate and dissuasive**

LMC LAW

SO, WHAT DO YOU NEED TO DO?

- GPs, as Data Controllers, are accountable under GDPR and must actively demonstrate compliance (will likely be done via DPO), therefore must:

  - ***document flows of data from the practice;***
  - ***have internal data protection policies/procedures in place;***
  - ***Carry out DPIA when engaging in new data sharing arrangements or where new technologies will be used or any other types of processing resulting in high risk to data subjects;***
  - ***train staff re. compliance – be aware of security of data and access requirements re any volunteers/work placement students;***
  - ***Provide the contact details of the DPO to patients;***

cont…

LMC LAW

SO, WHAT DO YOU NEED TO DO? continued

- ***Have a robust privacy policy in place;***
- ***Ensure your DPO (or current Caldicott Guardian) is properly trained and not conflicted;***
- ***Put leaflets and posters in surgeries so that patients are reasonably informed;***
- ***Update your website;***
- ***Make sure you review your new current registration processes;***
- ***Some good news… if you are performing well in IG toolkit this is a good start. 2016/17 IGT does not specifically tackle GDPR requirements and is in the process of being updated but is a good starting point to show compliance;***
- ***You need to be able to demonstrate to the ICO that you have made all reasonable efforts to comply with GDPR, including using best practice procedures, e.g. PIA***

LMC LAW

OTHER USEFUL INFORMATION

Contact details:
shaneebaker@lmclaw.co.uk
clairepye@lmclaw.co.uk
niobe.menelaou@lmclaw.co.uk
Tel: 07788 313582

LMC LAW