Information Governance Alliance

THE EU GENERAL DATA PROTECTION REGULATION: THE KEY POINTS FOR GPS

Contents

1 Introduction

This advice note has been written for GPs. It provides an overview of the General Data Protection Regulation (GDPR), highlights some key points, includes a checklist to help with preparation for the GDPR and provides links to further more detailed but relevant guidance.

The GDPR comes into full effect on 25 May 2018. It, coupled with a new UK Data Protection Act (DPA 2018), will replace the existing data protection law. The new law will also apply after Brexit.

As the new DPA 2018 is still undergoing Parliamentary scrutiny this advice note refers mainly to the GDPR because its provisions are set. The document will be updated once the DPA 2018 comes into effect.

2 General advice

In essence the new law takes the existing approach to data protection and strengthens it. For example, good practice under the DPA, such as Privacy Impact Assessments becomes mandatory in certain circumstances under the GDPR (in the form of Data Protection Impact Assessments (DPIAs)).

If you already meet the requirements of the current law then you are in a good place to meet the new GDPR standards. Even if you are not in this position there is a lot of material and support available to help you prepare for the GDPR.

There is also a locally commissioned Information Governance (IG) support service as part of 'core and mandated' GP IT Operating Model arrangements. You should use this service to help with your GDPR compliance. The details can be found within an Addendum to the 2016-18 GP IT Operating Model.

3 Myths

Understandably with a new high-profile law, myths have developed and been mixed with the truth about how the law will be applied and the consequences for individuals and organisations:

MYTH 1: Everything has to be sorted out and perfect for 25 May FALSE

Two quotes from the Information Commissioner Elizabeth Denham's blog best set this to rest:

"GDPR compliance will be an ongoing journey"; and "... if you can demonstrate that you have the appropriate systems and thinking in place you will find the ICO to be a proactive and pragmatic regulator aware of business needs and the real world".

Myth 2: Consent is needed for all processing of personal data FALSE

The GDPR sets a high standard for relying on consent, especially where that data is health related. However, it also provides alternative conditions that can be relied on instead of consent.

Myth 3: The Information Commissioner's Office (ICO) can levy fines of up to £17 million **TRUE**

However, the ICO has been a pragmatic and constructive regulator. It is likely that large fines will be only be used where organisations wilfully ignore their obligations and put data subjects (e.g. patients/individuals/citizens) at risk of harm because of their lack of legal compliance.

As the Information Commissioner has said: "Issuing fines has always been and will continue to be, a last resort."

4 Key issues

Data Protection Officer (DPO)

The GDPR applies to all organisations that use personal data. It further requires all 'public authorities' to appoint a Data Protection Officer (DPO). In the UK the definition of 'public authority' is taken from the Freedom of Information (FOI) Act 2000 and the FOI (Scotland) Act 2002. In short, if as a GP practice, you provide services to the NHS then your practice is likely to be a public authority and you will need to appoint a DPO.

Even if you do not consider that your practice is a public authority, the GDPR requires DPOs to be appointed where the controller processes 'large' (not defined) amounts of 'special category data' (formerly 'sensitive personal data'). This type of personal data includes health data. If you still consider that you do not require a formally appointed DPO, it would be good idea to have a data protection 'lead' or 'champion' in the practice.

The DPO should have data protection experience, be accountable to the senior levels of an organisation's management and fulfil the DPO tasks set out in the GDPR. However, a formal DPO can be a shared resource between organisations e.g. one individual might be the formal DPO for multiple GP practices.

In appointing a DPO, it is worth remembering that as this is new law it is untested. As such, there are no experts (no matter what people claim) on how the GDPR will work in practice (e.g. the ICO's decisions as the regulator and/or decisions of the higher courts). A Practice Manager, or one of their colleagues, can be appointed as DPO in addition to their existing roles as long as they have some data protection experience and are not the final decision taker about data use in the organisation (which would be seen as a conflict of interest).

The current ICO advice about an employee being a DPO is that this is acceptable; "... as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests".

Please see further IGA guidance about the DPO role.

Subject Access Requests

The GDPR makes two important changes to individuals' right of access to data about them. Firstly, the time period for complying with such requests has been reduced from 40 days to one calendar month.[1] Secondly, except for repeated requests, controllers will not be able to charge individuals for responding to these requests.

A further important point is that while the DPA 1998 specifies that requests must be made in writing, the GDPR has no such requirement. This means that in future requests could be made verbally. Whether a request is written or verbal you will need to check that the requestor is the person they say they are.

If you provide patients with online access to their medical record then it is likely that the changed approach to subject access requests will not be a burden on the practice because it is likely that it will reduce the number of requests.

Data Protection Fee

Under the current DPA, data controllers are required to notify the ICO that they are processing personal data and pay a fee (£35 for most organisations and £500 where the organisation's turnover is over £26 million and they employ more than 249 people).

On 25 May 2018 this arrangement will change. On that date the Data Protection (Charges and Information) Regulations 2018 will come into effect. In short they change the fee that is payable to either £40; £60 or (for large organisations) £2,900. The ICO has produced guidance that sets all this out in detail.

The current ICO plan is that the new fees will be phased in when an organisation's existing registration expires.

As this is the way that the ICO funds its data protection operations (they do not keep any fines imposed nor receive direct Government funding) it is an issue the ICO will act on. Currently 'non-notification' is a criminal offence which the ICO prosecutes. This will no longer be the case under the new Regulations but the ICO will have the power to directly levy a monetary penalty of up to £4,350.

Other issues

This advice is only a starter on the journey to fully meeting the GDPR's requirements. The following checklist will help you to identify further matters you will have to think about and then act on. Links to more detailed guidance are provided following the checklist.

1 The ICO position is that one calendar month starts on the day after receipt and ends on the same date of the next month (e.g. 2 January to 2 February), unless that date is a Saturday, Sunday or Bank Holiday, in which case it ends on the next working day. If that date does not exist because the following month has fewer days, it is the last day of the month (e.g. 31 January to 28 February).

In addition to the guidance there is a FAQ section on the IGA site and this is updated frequently as policy is developed and new issues are considered.

Support

The ICO has produced useful guidance which covers various specific GDPR requirements. The IGA has also produced specific health-focused guidance.

5 GDPR GP Checklist

This checklist is to support GP Practices to understand what they need to do to prepare for the new data protection law. It is not designed to provide all the answers; rather to get practices heading in the right direction in terms of meeting the new law's requirements. Following the checklist are specific links to further information connected to the checklist questions.

Part 1: The Basics

Question		Yes	No	Notes
1	Do you know about the General Data Protection Regulation (GDPR) and new Data Protection Act?			
2	Do you have a Data Protection Officer?			
3	Do you know where to find Information Governance (IG) support?			

Part 2: What to do next

Familiarise yourself with the GDPR		The Information Commissioner's Office's (ICO) '12 Steps to take now' should be read before completing the checklist: And the 'GDPR checklist for data controllers' will help with the next stages of your preparation:		
4	Can you identify what information you hold (patients and staff) how it is used and shared?			
5	Do you know about the legal rights that patients and staff have over their personal data which you process?			
6	Are you ready to handle Subject Access Requests under the GDPR?			
7	Have you reviewed your practice's privacy notice/ how it communicates about the information the practice uses?			

8	Where relevant can your privacy notice be easily understood by a child aged 13 and over.			
9	Can you identify your GDPR lawful basis for processing personal data?			
10	Have you implemented 'Data protection by design and default' principles; ensuring data protection is 'built-in' from the start of new activities?			
11	Can you distinguish between 'consent' for confidentiality purposes and 'consent' that meets the requirements of the GDPR?			
12	Are you prepared to investigate and report a data breach within the time required by the GDPR?			

The checklist links

1	**General awareness**	IGA GDPR CEO Briefing and The ICO 12 Steps
2	**Data Protection Officer**	The ICO DPO Guidance and IGA DPO Guidance
3	**IG support**	Links in this advice note and local support under the GP IT Operating Model arrangements.
4	**The information you hold and use**	The ICO DP self-assessment for Data Controllers
5	**Legal rights of patients and staff**	The ICO Individual Rights
6	**Subject access requests**	The ICO Individual Rights – right of access
7	**Transparency/privacy notices**	The ICO Individual Rights – right to be informed and ICO Privacy Notices, Transparency and Control.
8	**Children's rights**	The ICO – Children's rights
9	**GDPR lawful basis for processing**	The ICO – Lawful basis for processing and IGA GDPR Lawful Processing
10	**Data protection by design and default**	The ICO Data Protection by Design and Default
11	**Consent**	IGA GDPR Consent
12	**Data breaches**	ICO – Personal Data Breaches