Leeds Clinical Commissioning Groups Partnership

General Data Protection Regulation (GDPR) Guidance for GP Practices

Version:	V0.1
Date issued:	August 2018
Author:	Steve Creighton

GDPR Guidance for GP Practices

Introduction

The new General Data Protection Regulation (GDPR) took effect on 25 May 2018 and will replace the Data Protection Act 1998 (DPA). The GDPR will still apply even after the UK leaves the European Union.

GPs have a responsibility to comply with legislation and implement the new advice and guidance. This guide sets out your responsibilities under the GDPR and the changes in practice that must be implemented to ensure compliance with the new regulations.

Although in general, the principles of data protection remain similar, there is greater focus on evidence based compliance, more extensive rights for data subjects (patients and staff) and higher penalties for non-compliance.

The GDPR Privacy Principles

The GDPR contains six Privacy Principles governing how data will be processed and used:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the individual.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Rights of Individuals

The GDPR provides increased rights for individuals to enable them to have a better understanding of and more control over their personal information.

The right to information	Details of how their data is being processed and access to their data free of charge.
The right to access	In addition to accessing their records, individuals are now entitled to know how long we will keep their records and how they are stored.
The right to rectification	The individual has the right to rectify any inaccuracies or incomplete data held about them.
The right to be forgotten	This does not apply to health as we have a legal obligation to retain patient records.
The right to restriction of processing	This means that without consent, we can only process the data for the reason it was collected.
The right to notification	This is a duty for practices to notify any third parties that they may have shared the individual's information with, if they exercise any of their rights that may be relevant to them. Practices must also notify individuals if there is a breach of their personal data that could result in a risk to their rights and freedoms. Individuals are also able to request details of anyone that has seen their personal data.
The right to data portability	The individual may ask for a copy of their data in electronic format. This is only applicable to automated processing.
The right to object	The individual can object to certain types of processing, for example direct marketing.
The right to appropriate decision making	Individuals have the right not to be subject to a decision based solely on automated processing. Please note: this is not applicable to health records as automated processes are used to guide treatment after due consideration by a clinician.

What are the risks?

Data breaches and Infringement of the GDPR

Practices can be fined for any personal data breach. Personal data is information about individuals, including patients and staff. A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In addition fines may be imposed for any infringement of the GDPR, for example not appointing a Data Protection Officer.

Fines

Under the GDPR, fines for data breaches and non-compliance with the regulations are increasing, meaning any breach or infringement of the regulations could cost the practice more:

Maximum fine under the Data Protection Act (previous legislation)	**Maximum fine now under the GDPR (new data protection legislation)**
£500,000	**€20 million** or **4% of annual global turnover** (whichever is greater)

Summary of Changes

Legislation under Data Protection Act (up until 24 May 2018)	**New Legislation from 25 May 2018 under GDPR**
Only applied to the UK.	Applies to the whole of the EU and also to any global company which holds data on EU citizens.
Enforced by the Information Commissioner's Office (ICO).	Compliance will be monitored and enforced by the ICO in the UK, with each European country having its own Supervisory Authority.
Non-compliance could result in fines of up to £500,000.	The potential penalties for non-compliance are more severe, with fines of up to €20 million or 4% of the business's annual global turnover.
Under the previous legislation there is no need for a business to have a dedicated Data Protection Officer (DPO).	A Data Protection Officer (DPO) is mandatory for any business or organisation where the processing of information is carried out by a public authority or body (note- GP practices are "Public Bodies"); where the core activities of the data controller or the data processor consist of processing operations which require regular and systematic monitoring of individuals' information on a large scale (for example, health care).

Legislation under Data Protection Act (up until 24 May 2018)	New Legislation from 25 May 2018 under GDPR
Businesses were under no obligation to report data breaches although they were encouraged to do so.	Any serious data breach must be reported to the Information Commissioner's Office by the Data Protection Officer within 72 hours of the breach being identified.
There was no requirement for an organisation to remove all data they hold on an individual.	An individual will have the 'Right to erasure' – which applies to all data including internet records with all information being permanently removed. However, this is not applicable to health records (unless in accordance with the Information Governance Alliance guidance on retention periods).
Privacy Impact Assessments (PIAs) were not a legal requirement under the DPA.	Data Protection Impact Assessments (DPIAs) will be mandatory and must be carried out when there is a high risk to the freedoms of the individual. A DPIA helps an organisation to ensure they meet an individual's expectation of privacy.
Data collection did not necessarily require an opt-in under the current Data Protection Act.	The need for consent underpins GDPR. In respect of health we are not reliant on consent for processing of data, however there remains the need to request consent to share personal data outside the practice where it is not required for the health and welfare of the individual. The ability to withdraw consent must be as easy as it is to give consent.
A Privacy Notice was required, although no clear guidance was provided on the content.	A Privacy Notice must provide transparent information about the use and purpose of the data collected and also provide individuals with details of their rights under the GDPR. The Privacy Notice must be in a clear and accessible format.
Individuals' rights included the right to access any data we held about them, which we could provide at a cost of up to £50 and must have been provided within 40 calendar days.	Individuals' rights include the right to access any data we hold about them, which we must provide free of charge and within one calendar month (except in exceptional circumstances).

Requirements and Actions for GP Practices

Patient Information Leaflets

All Practices should update their patient information leaflets to include GDPR information. This guidance will inform patients of the reasons why their GP Practice use their information and signposts them to where they can find more information about how their data is used.

“How we use your personal information” leaflet

All practices should display ‘How we use your personal information’ leaflets in patient areas. A copy of this leaflet can also be given to every new patient at their first appointment.

Consent

Following the principles within the General Data Protection Regulation (GDPR), GP Practices do not generally rely on consent for processing patient and staff information for the purposes of the provision of publicly funded services (e.g. services commissioned by the NHS and the CCG), such as:

- Provision of health or social care or treatment;
- Medical diagnosis;
- Preventative or occupational medicine;
- Management of health or social care systems and services, carried out by, or under the supervision of health professional or another person, who in the circumstances owes a duty of confidentiality under an enactment or rule of law;
- Processing of payroll and other payments such as expenses; to inform staff about matters such as pensions; for legal reasons; for audits and to ensure that accurate references are given.

Consent is required however if we are going to share information about the individual with third parties outside of their health or social care needs; for example, subject access requests. It must be as easy for individuals to withdraw consent as it is to give consent.

Data Breach / Information Governance (IG) Incident

It is a GP Practice’s responsibility to notify the Information Commissioner’s Office (ICO) of serious data breaches within 72 hours of becoming aware of the breach.

Failure to do so could result in a fine of €10 million or 2% of the organisation’s annual turnover (whichever is larger) for not reporting the breach; as well as a fine of up to €20 million or 4% of annual turnover (whichever is larger) should GP Practices be found in breach of the Regulation.

Any actual or potential breaches of confidential information (including personal information) must be immediately reported as an incident on Datix and if appropriate be reported to the ICO via the Data Security Toolkit

The Data Protection Officer (DPO) and CCG IG team will be notified via Datix of all IG incidents reported and can determine whether an incident needs to be reported to the Information Commissioner’s Office (ICO).

Subject Access Requests (SARs)

Individuals (patients and staff) are entitled to request a copy or to view any information we hold about them; this includes patient or staff records, emails, complaints, incidents etc.

The GDPR provides more rights to the individual, including changes in the way we process requests for information:

- The timeline for completing information requests has reduced from 40 days to one month;
- All requests are free of charge, we are entitled to charge only in exceptional circumstances;
- When responding to personal requests we must provide our purpose for processing the data, the categories of data being processed and who the data is shared with.

Contracts with Third Party Organisations

The GDPR requires that organisations undertake due diligence on any third parties with which they share individuals' personal data to ensure that the third parties are compliant with the GDPR.

GP Practices should carry out due diligence for any contracts, arrangements and sharing agreements that they may hold independently (i.e. anything set up by practices themselves) to ensure partners are compliant with the GDPR. The suggested text for this letter is shown below:

Dear Account Manager

Subject matter: Compliance with the EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018. As part of our preparations we are conducting due diligence on all suppliers with which we share individuals' personal data to make sure they, and therefore we, are compliant.

We would appreciate it if you could answer the following questions to help us do this:

- What action are you taking to prepare for the GDPR?
- What technical and organisational security measures do you have in place to protect personal data?
- What policies and procedures do you have in place to protect personal data?
- How secure are your systems?
- Do you have any information management accreditation?

We would be grateful for your response as soon as possible

Data Privacy Impact Assessment (DPIA)

Under the GDPR it is mandatory to carry out a DPIA where the processing of data may result in a high risk to the rights and freedoms of individuals, for example the introduction of new information systems. If you require guidance from the, the CCG IT team can provide a DPIA form and assistance in completing it. Failure to carry out a DPIA in the appropriate circumstances could result in a fine of up to €10 million or 2% of our annual turnover, whichever is the greatest.

Key Roles and Responsibilities

The key roles for ensuring compliance with information governance regulations are set out below:

Role	Description	Name/Job Title
Data Controller	Data controllers of personal data are those who determine; the purposes for which that personal data are or will be processed; and the way in which that personal data are or will be processed.	
Data Processor	Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.	
Data Protection Officer (DPO)	The role of the DPO is to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws. The DPO will be the first point of contact for the Information Commissioner's Office (ICO) and for individuals whose data is processed. The DPO will be responsible for reviewing compliance, but is not responsible for compliance; this remains the responsibility of the Data Controller.	
Caldicott Guardian	A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about people who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.	