AberGP

PRIVATE GENERAL PRACTICE

UK GDPR Policy

Table of Contents

Introduction 4
Policy statement 4
Status 4
Data protection 4
Data protection by design and default 4
Roles of data controllers and processors 5
Data controller 5
Data processor 5
Data subjects' rights 6
Right to be informed 6
Right of access 6
Right to rectification 6
Right to erasure 6
Right to restrict processing 7
Right to data portability 7
Right to object 7
Rights in relation to automated decision making and profiling 7
Subject access requests 8
Recognising subject access requests (SAR) 8
Responding to a subject access request 8
Fees 8
Verifying the subject access request 8
Supplying the requested information 8
Third party requests 9
Requests from solicitors 9
Requests from insurers 9
Refusing to comply with a SAR 9
Data breaches 10
Data breach definition 10
Reporting a data breach 10
Notifying a data subject of a breach 11
Consent 11
Obtaining consent 11
Parental consent 11
Data mapping and Data Protection Impact Assessments 12

Data mapping 12
Data mapping and the Data Protection Impact Assessment 12
Data Protection Impact Assessment 12
Data Protection Impact Assessment process 13
Information asset register 13
Annex A – UK GDPR checklist 14

Introduction

Policy statement

The UK General Data Protection Regulation (UK GDPR herein) is incorporated in the Data Protection Act 2018 (DPA18) at Part 2, Chapter 2 and applies to all organisations in the UK (with the exception of law enforcement and intelligence agencies). AberGP must be able to demonstrate compliance at all times. Understanding the requirements of the UK GDPR will ensure that the personal data of both staff and patients is protected accordingly.

To help to maintain compliance with the UK GDPR a checklist is available at Annex A.

Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

Data protection

Data protection by design and default

The Information Commissioner's Office (ICO) advises that the UK GDPR requires this organisation to put in place appropriate technical and organisational measures to implement the data principles effectively; this is data protection by design and default.

Data protection by design is about considering data protection and privacy issues upfront, in everything that the organisation does. Data protection by default requires this organisation to only process the data that is necessary to achieve a specific purpose.

This organisation will demonstrate data protection by design and default by:

- Conducting a Data Protection Impact Assessment (DPIA)
- Ensuring there are privacy notices on the website and in the waiting rooms which are written in simple, easy-to-understand language
- Adhering to Articles 25(1) and 25(2) of the UK GDPR
- Processing data only for the purpose(s) intended
- Ensuring consent is obtained from the data subject prior to data being processed
- Providing patients with access to their data on request (Subject Access Requests)

- Ensuring patients consent to access of their data by third parties
- Processing data in a manner that prevents data subjects being identified unless additional information is provided (using a reference number as opposed to names – pseudonymisation)

Roles of data controllers and processors

Data controller

The ICO defines a data controller as a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers are responsible for the compliance of their processor(s).

This organisation is the data controller for the data it holds about its patients. The organisation must ensure and be able to demonstrate compliance with Article 5 of the UK GDPR which relates to the seven key principles of processing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Data processor

The ICO defines a data processor as a person, public authority, agency or other body which processes personal data on behalf of the controller. Processors must ensure that processing conforms to Article 6 of the UK GDPR:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, when the data subject is a child

At this organisation, all staff are classed as data processors as their individual roles will require them to access and process personal data.

Data subjects' rights

Right to be informed

The ICO explains that Articles 13 and 14 of the UK GDPR specify what individuals have the right to be informed about; this is referred to as 'privacy information'.

Right of access

This organisation ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Organisation website
- Organisation information leaflet

To comply with the UK GDPR, all privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the UK GDPR.

The ICO advises that the right of access is commonly referred to as subject access and gives individuals the right to obtain a copy of their personal data, as well as other supplementary information this organisation holds about them.

Right to rectification

As stated by the ICO, under Article 16 of the UK GDPR, data subjects have the right to have inaccurate personal data rectified and/or incomplete personal data completed. At this organisation, should a clinician enter a diagnosis that is later proved incorrect, the medical record should retain both the initial diagnosis and the subsequent accurate diagnosis with text to make it clear that the diagnosis has been updated.

Patients can exercise their right to challenge the accuracy of their data and request that this is corrected. Should a request be received, the request should state the following:

- What is believed to be inaccurate or incomplete
- How this organisation should correct it
- If able to, provide evidence of the inaccuracies

Detailed guidance from the ICO can be accessed here.

Right to erasure

The ICO explains that, in accordance with Article 17 of the UK GDPR, data subjects have the right to have personal data erased (this is also known as the right to be forgotten). This right permits a data subject to request that personal data is deleted in situations when there is no compelling reason to retain the data. The right is not absolute and only applies in certain circumstances.

Detailed information can be found at section 4.11 of the BMA Access to health records guidance.

When this organisation has shared information with a third party, there is an obligation to inform the third party about the data subject's request to erase their data providing it is achievable and reasonably practical to do so.

Right to restrict processing

The ICO states that Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data. This applies in certain circumstances, with the aim being to enable the individual to limit the way this organisation processes (uses) their data. This right can be used as an alternative to the right to erasure.

Right to data portability

The ICO explains the right to data portability permits data subjects to receive and reuse their personal data for their own purposes and across different services.

Right to object

The ICO advises that, in accordance with Article 21 of the UK GDPR, individuals have the right to object to the processing of their personal data at any time. At this organisation, individuals are requested to provide specific reasons why they object to the processing of their data. If the reasons are not an absolute right, this organisation can refuse to comply.

Rights in relation to automated decision making and profiling

The ICO explains that Article 22 of the UK GDPR prevents this organisation from using solely automated decision making, this includes profiling.

Subject access requests

Recognising subject access requests (SAR)

The ICO states "An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact".

Staff at this organisation are to encourage the use of the SAR form (included in the Access to Medical Records Policy). However, they must accept that any requests that do not use the SAR form are to be processed.

Responding to a subject access request

The ICO advises that this organisation must respond to a SAR without delay and within one month of receipt of the request. This time limit may be extended by a further two months if the request is complex or multiple requests are received from the individual.

Should the request involve a large amount of information, this organisation will ask the individual to specify what data they require before responding to the request. The time limit for responding to the request is paused until clarification is received.

Fees

As stated by the ICO, this organisation is not permitted to charge a fee to comply with a SAR. However, a reasonable fee may be charged if the request is deemed to be manifestly unfounded or excessive, or if an individual requests further copies of their data.

Verifying the subject access request

The ICO explains that this organisation must satisfy itself that the identity of the requestor is known (or the identity of the person the request is made on behalf of). It is acceptable to request information to verify an individual's identity. Note, the timescale for responding to a SAR does not begin until the requested information has been received. The organisation's SAR form supports the data controller in verifying the request.

Supplying the requested information

ICO guidance explains that the decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided. It is considered good practice to establish the individual's preferred method before fulfilling their request.

Third party requests

This organisation, as a data controller, must be able to satisfy itself that the person requesting the data has the authority of the data subject. The responsibility for providing the required authority rests with the third party this organisation will request that third parties use the BMA and Law Society consent form.

Requests from solicitors

This organisation will receive SARs from third parties, such as solicitors, who have been authorised by a patient to make a SAR on their behalf. It is the responsibility of the third party to provide evidence that they are permitted to make a SAR on behalf of their client. If concern or doubt arises, this organisation will contact the patient to explain the extent of disclosure sought by the third party.

This organisation can then provide the patient with the data as opposed to directly disclosing it to the third party. The patient is then given the opportunity to review their data and decide whether they are content to share the information with the third party.

Requests from insurers

SARs are not appropriate should an insurance company require health data to assess a claim. The correct process for this at this organisation is for the insurer to use the Access to Medical Reports Act 1988 when requesting a GP report.

The BMA suggests the following fees are applicable:
- GP report for insurance applicants £104.00
- GP supplementary report £27.00

Refusing to comply with a SAR

As detailed by the ICO, this organisation will only refuse to comply with a SAR when exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the organisation will inform the individual of:
- The reasons why the SAR was refused
- Their right to submit a complaint to the ICO
- Their ability to seek enforcement of this right through the courts

Each request must be given careful consideration and, should this organisation refuse to comply, this must be recorded and the reasons for refusal justifiable.

Data breaches

Data breach definition

The ICO defines a data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclose of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Examples of data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a data controller or processor
- Sending personal data to an incorrect recipient
- Loss or theft of computer devices containing personal data
- Alteration of personal data without permission
- Loss of availability of personal data

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

Reporting a data breach

The ICO explains that the UK GDPR introduced a duty on all organisations to report certain types of data breach to the relevant supervisory authority (the ICO) within 72 hours of becoming aware of the breach. If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR states that those individuals must also be informed directly and without undue delay.

The above must be assessed on a case-by-case basis by the organisation's Data Protection Officer (DPO) and Senior Information Risk Officer (SIRO)/Caldicott Guardian. Therefore, a breach MUST be reported to the Information Governance Lead, DPO and SIRO/Caldicott Guardian within 24 hours of the organisation becoming aware of it so that an appropriate assessment can take place.

This organisation will report the breach using the Data Security and Protection Incident Reporting Tool. Article 33 of the UK GDPR outlines the information required when reporting a breach. The ICO explains this information must contain:

- A description of the nature of the breach, including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details for the DPO
- A description of the likely consequences of the data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects

Notifying a data subject of a breach

The ICO explains that if a breach is likely to result in a high risk to the rights and freedoms of individuals, then this organisation must inform those concerned directly and without undue delay and before notifying the ICO. One of the main reasons for doing so is to permit those affected to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, this organisation is to provide those affected with the following information in a clear, comprehensible manner:

- The circumstances surrounding the breach
- The details of the person who will be managing the breach
- Any actions taken to contain and manage the breach
- Any other pertinent information to support the data subject

Consent

Obtaining consent

The ICO states that consent must be unambiguous and involve a clear affirmative action (an opt-in). Consent is one of the lawful bases of processing and, if appropriate, this organisation is to offer people real choice and control over how their data is used. If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the organisation wants the data
- How the data will be used by the organisation
- The names of any third-party data controllers with whom the data will be shared
- Their right to withdraw consent at any time

All requests for consent are to be recorded, with the record showing:

- The details of the data subject consenting
- When they consented
- How they consented
- What information the data subject was told

Consent is to be clearly identifiable and separate from other comments entered into the healthcare record. Furthermore, this organisation must ensure that data subjects (patients) are fully aware of their right to withdraw consent at any time and must facilitate withdrawal as and when it is requested.

Parental consent

The DPA 2018 states that parental consent (in relation to personal data) is required for a child under the age of 13. Additionally, the principle of Gillick competence remains unaffected and parental consent is not necessary when a child is receiving counselling or preventative care. For further information refer to the Consent Guidance.

Data mapping and Data Protection Impact Assessments

Data mapping

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable this organisation to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared and where it is stored (including off-site storage if applicable).

The Register of Processing Activities (ROPA) details the process of data mapping at this organisation.

Data mapping and the Data Protection Impact Assessment

Data mapping is linked to the Data Protection Impact Assessment (DPIA) and, when the risk analysis element of the DPIA process is undertaken, the information ascertained during the mapping process can be used.

Data Protection Impact Assessment

The ICO explains that conducting a DPIA is a legal requirement for any type of processing, and a DPIA is the most efficient way for this organisation to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs.

In accordance with Article 35 of the UK GDPR, a DPIA should be undertaken when:

- A type of processing, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks
- Extensive processing activities are undertaken, including large scale processing of personal and/or special data

DPIAs are to include the following:

- A description of the processing operations, including the purpose of processing
- An evaluation of the need for the processing in relation to the purpose
- An assessment of the associated risks to the data subjects
- Existing measures to mitigate and control the risk(s)
- Evidence of compliance in relation to risk control

It is considered best practice to undertake DPIAs for existing processing procedures to ensure that this organisation meets its data protection obligations. DPIAs are classed as "live documents" and processes should be reviewed continually. As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

Data Protection Impact Assessment process

The DPIA process is illustrated in diagrammatic form below:

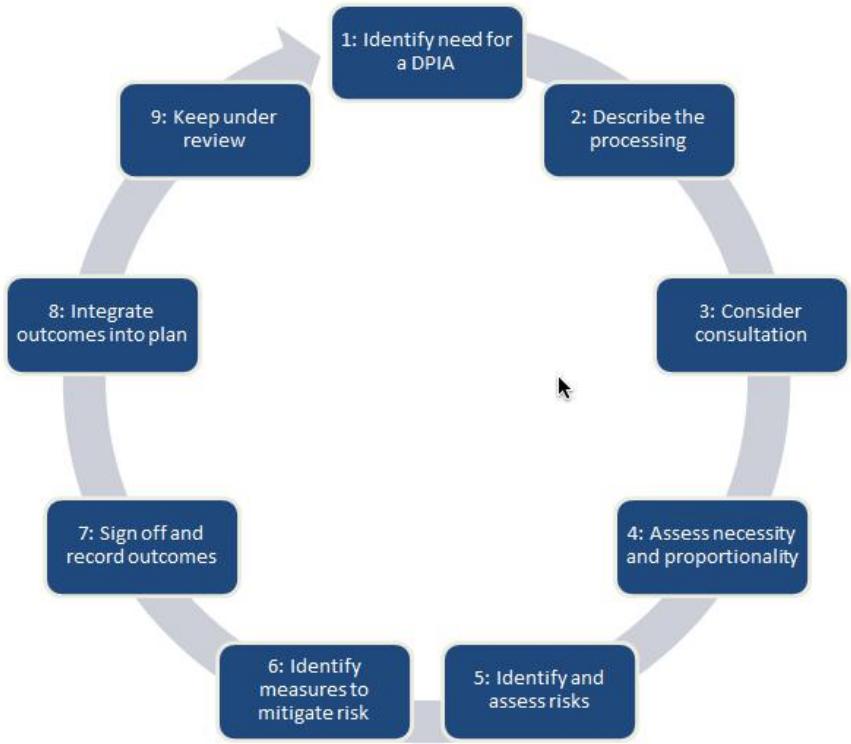

Image source: ico.org.uk

Information asset register

The ICO advises that an information asset register (IAR) records assets, systems and applications that are used for processing or storing personal data across this organisation. The IAR is to be kept up to date, detailing all information assets (software and hardware), including:

- Asset owners
- Asset location
- Retention periods
- Existing security measures

The register is to be reviewed regularly to ensure it remains extant, and best practice is to risk-assess assets within the register, conducting physical checks to make certain the hardware asset inventory remains accurate.

This organisation will use the Information Asset Register template.

Annex A – UK GDPR checklist

This checklist has been designed to support managers in ensuring compliance with the UK GDPR.

Creating a culture of awareness	
All staff need to be aware of the UK GDPR requirements. • It is essential that they have an understanding of the UK GDPR • Have you shared the organisation's UK GDPR policy with them or signposted them to further information, i.e., ico.org.uk?	
Action complete (✓ or ✗)	

Understanding the information flow	
The organisation must understand why, whose, what, when and where personal data is processed. • Conducting a data mapping exercise will enable organisations to do this • Data mapping is not a one-person task; all staff should be involved, enabling the wider gathering of accurate information	
Action complete (✓ or ✗)	

Data Protection Impact Assessment (DPIA)	
The DPIA is the most efficient way for the organisation to meet its data protection obligations. DPIAs are mandatory in accordance with Article 35 of the UK GDPR and should be undertaken when: • A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations which present similar high risks • Extensive processing activities are undertaken, including large scale processing of personal and/or special data Have DPIAs been completed? Best practice is to undertake DPIAs for existing processes to ensure that data protection obligations are met.	
Action complete (✓ or ✗)	

Updating privacy information	
All data subjects must understand how their data will be used. • Have you updated your practice privacy notice and are all staff aware of the changes? • Have you displayed the privacy notice in prominent positions such as the waiting room, consulting rooms and website and updated the organisation's information leaflet? • Is your privacy notice in a language that is understandable to all patients? • Does it comply with Articles 12, 13 and 14 of the UK GDPR?	
Action complete (✓ or ✗)	

The rights of the data subject	
All data subjects have rights. Has this been communicated or is information displayed to reflect this? Does it include the: • Right of access • Right to erasure (or right to be forgotten) • Right to data portability • Right to object • Right to rectification • Right to restriction of processing • Right to notification • Right not to be subject to automated decision-making (including profiling)	
Action complete (✓ or ✗)	

Subject access requests	
All data subjects have a right to access their data and any supplementary information held. Does the practice policy reflect the UK GDPR and do staff understand: • There is no fee applicable for SARs • The response time is one calendar month • Requests can be refused, but must be fully justified • Requests can be received by email	
Action complete (✓ or ✗)	

Processing personal data	
Do data processors within the organisation understand that they are responsible for the processing of data on behalf of the data controller? Do all processors know that one of the following must apply? • The data subject has given consent to the processing of his/her personal data for one or more specific purposes • Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract • Processing is necessary for compliance with a legal obligation to which the controller is subject • Processing is necessary in order to protect the vital interests of the data subject or another natural person • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller • Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child	
Action complete (✓ or ✗)	

Consent	

• Do current processes for obtaining consent reflect the UK GDPR?
• Do staff know that they must explain to data subjects:
  ○ Why the organisation wants the data
  ○ How the data will be used by the organisation
  ○ The names of any third party data controllers with whom the data will be shared
  ○ Their right to withdraw consent at any time
• Are staff aware that the Data Protection Act (DPA18) states that parental consent is required for a child under the age of 13; Gillick competence remains unaffected	

Action complete (✓ or ✗)	

Data breaches	
What are the current procedures to detect and report data breaches? • Do staff know what a data breach is? • What is the reporting process? • Is there a process to notify data subjects of a breach affecting them? • How are data breaches recorded; who is responsible for this? • Does the practice policy include data breaches and responsibilities?	
Action complete (✓ or ✗)	