General Data Protection Regulation Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	06/03/2019	SB	SB	

Table of contents

1 Introduction

1.1 Policy statement

The EU General Data Protection Regulation (GDPR herein) came into force on 25 May 2018; the Data Protection Act 2018 (DPA 2018) is to be read in conjunction with the GDPR. The GDPR applies to all EU member states and Staines Road Surgery must be able to demonstrate compliance at all times. Understanding the requirements of the GDPR will ensure that personal data of both staff and patients is protected accordingly.

1.2 Status

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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.

1.3 Training and support

The practice will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

This document applies to all employees, partners and directors of the practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are encouraged to use it.

2.2 Why and how it applies to them

All personnel at Staines Road Surgery have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the GDPR.

The practice 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 in regard to the individual protected characteristics of those to whom it applies.

3 Definition of terms

3.1 Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) is a complete data protection system, covering general data, law enforcement data and national security data.

3.2 Data Protection Officer

An expert on data privacy, working independently to ensure compliance with policies and procedure.

3.3 Data Protection Authority

National authorities tasked with the protection of data and privacy.

3.4 Data Controller

The entity that determines the purposes, conditions and means of the processing of personal data.

3.5 Data Processor

The entity that processes data on behalf of the Data Controller.

3.6 Data Subject

A natural person whose personal data is processed by a controller or processor.

3.7 Personal data

Any information related to a natural person or ‘data subject’.

3.8 Processing

Any operation performed on personal data, whether automated or not.

3.9 Recipient

The entity to which personal data is disclosed.

4 The build-up to the GDPR

4.1 Background

The GDPR is based on the 1980 Protection of Privacy and Transborder Flows of Personal Data Guidelines, which outlined eight principles:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

4.2 NHS Digital

The Information Governance Alliance (IGA) is the authority that gives advice and guidance on the rules governing the use and sharing of healthcare-related information for the NHS. NHS Digital provides up-to-date information regarding the GDPR as well as a range of useful guidance documentation.[1]

4.3 Aim of the GDPR

The GDPR was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way in which organisations across the region approach data privacy.[2]

4.4 Brexit and the GDPR

Despite leaving the EU, the GDPR will still be enforced as it applies prior to the UK leaving the EU. The Regulation became applicable as law in the UK as of the 25th May 2018.

4.5 GDPR and DPA18

To ensure that organisations have a complete overview of the legislation, it will be necessary to view the GDPR and DPA 2018 side by side.[3]

5 Roles of data controllers and processors

5.1 Data controller

At Staines Road Surgery the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. She should be able to demonstrate compliance and is responsible for making sure data is:[4]

[1] NHS Digital GDPR guidance
[2] EU GDPR overview
[3] IGA The General Data Protection Regulation What's New
[4] Article 5 GDPR Principles relating to processing of personal data

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 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

The data controller at Staines Road Surgery is Sarah Butler; they are responsible for ensuring that all data processors comply with this policy and the GDPR.

5.2 Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:[5]

- 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 controller
- Processing is necessary for the purposes of the legitimate interests pursued by the 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

At Staines Road Surgery all staff are classed as data processors as their individual roles will require them to access and process personal data.

[5] Article 6 Lawfulness of processing

6 Access

6.1 Data subject's rights

All data subjects have a right to access their data and any supplementary information held by Staines Road Surgery Data subjects have a right to receive:

- Confirmation that their data is being processed
- Access to their personal data
- Access to any other supplementary information held about them

Staines Road Surgery ensures that all patients are aware of their right to access their data and has privacy notices displayed on the practice website.

To comply with the GDPR, all practice 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 GDPR.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third-party access, e.g. for solicitors and insurers, under the GDPR.

6.2 Fees

Under the GDPR, Staines Road Surgery is not permitted to charge data subjects for initial access; this must be done free of charge. In instances where requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive", a reasonable fee may be charged. However, this does not permit the practice to charge for all subsequent access requests.[6]

The fee is to be based on the administrative costs associated with providing the requested information.

6.3 Responding to a data subject access request

In accordance with the GDPR, data controllers must respond to all data subject access requests within one month of receiving the request (previous subject access requests had a response time of 40 days). It is the guidance of the BMA that a universal approach is applied and a 28-day response time implemented.[6]

In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.

6.4 Verifying the subject access request

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. The use of the practice Subject Access Request (SAR) form supports the data controller in verifying the request. In addition, the data

[6] BMA Guidance – Access to health records

controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e. driving licence or passport.

6.5 THIRD-PARTY REQUESTS

Third-party requests will continue to be received following the introduction of the GDPR. The data controller must be able to satisfy themselves 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 and is usually in the form of a written statement or consent form, signed by the data subject. A standard consent form has been issued by the BMA and Law Society of England and Wales and Staines Road Surgery will request that third parties complete this form.

6.6 Requests from insurers[6]

The Information Commissioner's Office (ICO) refers to the use of SARs to obtain medical information for insurance purposes as being in fact an abuse of access rights, and the processing of full medical records by insurance companies risks breaching the GDPR.

Staines Road Surgery will ensure consent forms are signed by patients and verify the information being requested with the patient before sending.

Staines Road Surgery will advise insurers to use the Access to Medical Reports Act 1988 when requesting a GP report. The following fees are applicable:[7]

- GP report for insurance applicants £104.00
- GP supplementary reports £27.00

7 Data breaches

7.1 Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.[8] Examples of data breaches include:

- Unauthorised third-party access to data
- Loss of personal data
- Amending personal data without data subject authorisation
- The loss or theft of IT equipment which contains personal data
- Personal data being sent to the incorrect recipient

7.2 Reporting a data breach

[7] BMA Guidance – Fees for insurance reports and certificates
[8] ICO – Personal data breaches

Any breach that is likely to have an adverse effect on an individual's rights or freedoms must be reported. In order to determine the requirement to inform the ICO, to notify them of a breach, the data controller is to read this supporting guidance. Breaches must be reported without undue delay or within 72 hours of the breach being identified.

When a breach is identified and it is necessary to report the breach, the report is to contain the following information:

- Organisation details
- Details of the data protection breach
- What personal data has been placed at risk
- Actions taken to contain the breach and recover the data
- What training and guidance has been provided
- Any previous contact with the Information Commissioner's Office (ICO)
- Miscellaneous support information

The ICO data protection breach notification form should be used to report a breach. Failure to report a breach can result in a fine of up to €10 million.[9]

The data controller is to ensure that all breaches at Staines Road Surgery are recorded; this includes:

- Documenting the circumstances surrounding the breach
- The cause of the breach; was it human or a system error?
- Identifying how future incidences can be prevented, such as training sessions or process improvements

7.3 Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e. a breach that is likely to have an adverse effect on an individual's rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity 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, the data controller at Staines Road Surgery is to provide the data subject 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

[9] ICO Personal data breaches

8 Data erasure

8.1 Erasure

Data erasure is also known as the “right to be forgotten”, which enables a data subject to request the deletion of personal data where there is no compelling reason to retain or continue to process this information. It should be noted that the right to be forgotten does not provide an absolute right to be forgotten; a data subject has a right to have data erased in certain situations.

The following are examples of specific circumstances for data erasure:

- Where the data is no longer needed for the original purpose for which it was collected
- In instances where the data subject withdraws consent
- If data subjects object to the information being processed and there is no legitimate need to continue processing it
- In cases of unlawful processing
- The need to erase data to comply with legal requirements

The data controller can refuse to comply with a request for erasure in order to:

- Exercise the right for freedom of information or freedom of expression
- For public health purposes in the interest of the wider public
- To comply with legal obligations or in the defence of legal claims

9 Consent

9.1 Appropriateness

Consent is appropriate if data processors are in a position to “offer people real choice and control over how their data is used”.[10] The GDPR states that consent must be unambiguous and requires a positive action to “opt in”, and it must be freely given. Data subjects have the right to withdraw consent at any time.

9.2 Obtaining consent

If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the practice wants the data
- How the data will be used by the practice
- The names of any third-party 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

[10] ICO Consent

- 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. At Staines Road Surgery it is the responsibility of the data controller Sarah Butler to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (patients) are fully aware of their right to withdraw consent, and must facilitate withdrawal as and when it is requested.

9.3 Parental consent

Whilst the GDPR states that parental consent is required for a child under the age of 16, the DPA 2018 will reduce this age to 13 in the UK. Additionally, the principle of Gillick competence remains unaffected; nor is parental consent necessary when a child is receiving counselling or preventative care.

10 Data mapping and Data Protection Impact Assessments

10.1 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 Staines Road Surgery 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.

Annex A details the process of data mapping at Staines Road Surgery

10.2 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 mapping is not a one-person task; all staff at Staines Road Surgery will be involved in the mapping process, thus enabling the wider gathering of accurate information.

10.3 Data Protection Impact Assessment

The DPIA is the most efficient way for Staines Road Surgery 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 GDPR, DPIA should be undertaken where:

- 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; then 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 process, including the purpose
- 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 Staines Road Surgery 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.

10.4 DPIA process

The DPIA process is formed of the following key stages:

- Determining the need
- Assessing the risks associated with the process
- Identifying potential risks and feasible options to reduce the risk(s)
- Recording the DPIA
- Maintaining compliance and undertaking regular reviews

A separate DPIA policy is enforce at Staines Road Surgery

11 Summary

Given the complexity of the GDPR, all staff at Staines Road Surgery must ensure that they fully understand the requirements within the Regulation. Understanding the Regulation will ensure that personal data at Staines Road Surgery remains protected and the processes associated with this data are effective and correct.

Regular updates to this policy will be applied when further information and/or direction is received.

Annex A – The data-mapping process

WHY is personal data processed?	
Personal data is defined as any information relating to a natural person or "data subject"; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[11]	
Personal data may be used for the following reasons:	
Staff administration	**Patient records**
• Contact details • Contracts, DBS applications • Pay, tax, pensions etc. • Application forms for training etc. • CCTV • Use of IT • Minutes of meetings	• Contact details • Health records • Referrals • Prescriptions • CCTV • Online service/practice apps • PPG membership, minutes etc.
List the reasons why personal data is processed:	
- Patient information is used for the purposes of Patient Direct Care. - We can disclose information if required by law, if it is in the publics best interest or if the patient gives consent to do so for a third party. - Patient information may be required to support national research, however, consent will always be obtained from the patient first. - Information regarding staff personal data can be found in the staff contract. - In the case of Locum staff being used to cover annual leave or sickness, all necessary paperwork will be obtained to ensure their ability and right to work in an NHS environment and specific to their role.	

[11] GDPR Article 4 Definitions

WHO – whose personal data is processed?
Having identified why personal data is processed, use those reasons to determine whose personal data is processed. Patients Staff members

Personal data may be processed for the following data subjects:	
Staff	**Patients**
• Current / former • Locums / temps / consultants • Potential employees • Volunteers	• Current / previous • Carers / relatives / guardians • Third-party representatives
Contractors/suppliers	**Other**
• Cleaners • Pharmacy • Equipment servicing/repair	• Reps • Guest speakers • Trainers

List whose personal data is processed:
As above

<table>
<tr><th colspan="2">WHAT personal data is processed?</th></tr>
<tr><td colspan="2">Having identified why and whose personal data is processed, use those reasons to determine what personal data is processed. The source of the data and the legal basis (why it was provided) must also be recorded.</td></tr>
<tr><th colspan="2">Types of personal data that may be processed:</th></tr>
<tr><th>Staff</th><th>Patients</th></tr>
<tr><td>Name / address
Email / phone number etc.
Occupational health information
Training records
Employment information / appraisals etc.
ID verification (passport / driving licence etc.)
Necessary details for payroll</td><td>Name / address
Email / phone number etc.
Healthcare information
ID verification (passport / driving licence etc.)</td></tr>
<tr><th>Source</th><th>Legal basis</th></tr>
<tr><td>Data subject
Third party
Other (specify)</td><td>Legal obligation / lawful function
Consent
Contract related
Legitimate interest of the data controller</td></tr>
<tr><th colspan="2">WHEN is personal data processed?</th></tr>
<tr><td colspan="2">Data is processed when necessary;
Following changes or updates to the data held.
When requested via an SAR</td></tr>
<tr><th colspan="2">Types of personal data that may be processed:</th></tr>
<tr><th>Staff</th><th>Patients</th></tr>
<tr><td>Receiving, transferring or updating the following:
Name / address
Email / phone number etc.
Occupational health information
Training records
Employment information / appraisals etc.
ID verification (passport / driving licence etc.)</td><td>Receiving, transferring or updating the following:
Name / address
Email / phone number etc.
GP2GP / medical records
Results, letters etc.
ID verification (passport / driving licence etc.)</td></tr>
<tr><th>Sharing and disclosure</th><th>Sharing and disclosure</th></tr>
<tr><td>Appraisal
References
Awards and recommendations
OH
Incident reports / forms
Business cases
Insurance and banking</td><td>Referrals
Results
Letters to other service providers</td></tr>
<tr><th>Retention</th><th>Retention</th></tr>
</table>

• In accordance with the current retention schedule	• In accordance with the current retention schedule

WHERE is personal data processed?		
Having identified why, whose, what and when personal data is processed, use those reasons to determine where personal data is processed. The source of the data and the legal basis (why was it provided) must also be recorded.		
Types of personal data that may be processed:		
Staff	**Patients**	
• Name / address • Email / phone number etc. • Occupational health information • Training records • Employment information / appraisals etc. • ID verification (passport / driving licence etc.)	• Name / address • Email / phone number etc. • Healthcare information • ID verification (passport / driving licence etc.)	
Manual records	**Electronic records**	**IT system**
• Lloyd George • Staff files • Hard copies of prescriptions etc.	• Locally established databases • Vision	• Fixed • Remote servers • Intranet
Manual: **Lloyd Georges - Kept securely on sight at surgery. Only used in instances as stated above for data processing.** **Staff Files – Kept securely on sight.** **Prescriptions – Processed at the Surgery and sent on via the patients chosen route i.e – to pharmacy or collected by patient.**		
Electronic records: All held securely on clinic system – Aeros, Vision		
IT system: All security measures in place to ensure Data is protected.		