|  |
| --- |
| logoDorridge Surgery**General Data Protection Regulation Policy** |
| Guidelines Prepared by:Amanda ShakespearePractice Manager | Guidelines Approved by:Dr John Davenport | Date Next Review Due: | 21/5/202022/1/2022 |  |
| Date Prepared:21/05/2018 | Date Approved:21/5/2018 | Date Review Takes Place: | 22/1/2020 |  |

# Introduction

## Policy statement

The EU General Data Protection Regulation (GDPR) was approved in 2016 and will become directly applicable as law in the UK from 25th May 2018. The current Data Protection Bill, which will become the Data Protection Act 2018 (DPA18), fills in the gaps in of the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit – it is expected that the DPA18 will ensure continuity by putting in place the same data protection regime in be UK law pre- and post- Brexit, to create a data protection regime in the UK equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

Understanding the requirements of the GDPR will ensure that personal data of both staff and patients is protected accordingly. Hobs Moat Medical is committed to ensuing adherence to these regulations and undertakes to ensure all staff are given relevant training and that data is protected.

The Practice has an obligation to self assess and self declare against the Information Toolkit hosted by NHS Digital. This maps IG toolkit requirements to GDPR.

## Status

This document and any procedures contained within it are contractual and therefore all staff are required to comply with its contents.

 **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.

**Scope**

## Who it applies to

This document applies to all employees and partners of the practice. This also applies to other individuals performing functions in relation to the practice, such as agency workers, locums and contractors.

## Why and how it applies to them

All personnel at Dorridge 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/DPA2018.

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.

# Definition of terms

## Data Protection Officer (DPO)

An expert on data privacy, working independently to ensure compliance with policies and procedure and who is knowledgeable about the way the organisation works.

Their responsibilities are

* Advising their colleagues on compliance.
* Training and awareness raising.
* Monitoring compliance, and carrying out audits.
* Providing advice regarding DPIAs.
* Taking a risk based approach to compliance.
* Being the main contact point with the ICO.
* Maintaining their own expert knowledge of data protection.

As a smaller organisation it is possible to appoint an external DPO or a DPO that is shared by several organisations

Our DPO is Paul Couldrey c/o PCIG Consulting Ltd –Should you need any assistance please contact us by either:

* Telephone - 0115 838 6770
* Email – info@pcdc.org.uk

## Data Protection Authority

This responsibility rests with the Information Commissioners Office (ICO)

## Data Controller

 A data controller:

* Is an individual or body with a legal identity (e.g. NHS Trusts, CCGs, GP Practices, Local Authorities)
* Determines the purposes for which personal data will be processed and/or
* Determines the way that the data is processed

Data controllers are required to comply with the Data Protection Principles and meet the other obligations imposed by the Data Protection Act.

## Data Processor

## A data processor can be anyone (other than an employee of the data controller) who processes the data on behalf of the data controller. the act imposes specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors. the data controller retains full responsibility for the actions of the data processor – if there is a data protection breach then the data controller remains responsible. the key obligation is that the processing by a data processor must be carried out under a written contract which requires the data processor to act only on instructions from the data controller. in the absence of a written contract a body will be a data controller in its own right and will need to meet all the requirements of the DPA.

## Data Subject

**Data subject** means an individual who is the **subject** of personal **data**. In other words, the **data subject** is the individual whom particular personal **data** is about.

## Personal data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people.

**Sensitive Personal Data**

The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Article 9 refers to

racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation

General Practice is allowed to process this data on the basis of Article 9, paragraph 2 sub section h

## Processing

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

## Recipient

The entity to which personal data is disclosed.

# The build-up to the GDPR

## 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

## 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. As a result of the imminent introduction of the GDPR, an NHS policy is being developed by the GDPR working group and will be published in due course.

NHS Digital provides up-to-date information regarding the GDPR as well as a range of useful guidance documentation.[[1]](#footnote-2)

The current IGA advice can be found [here](https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance)

## Aim of the GDPR

The **GDPR** is a set of EU laws that come into effect on May 25th 2018. The **purpose** of the **GDPR** is to provide a set of standardised data protection laws across all the member countries.

The laws aim to protect and empower all EU citizens’ data privacy and to reshape the way in which organisations across the region approach data privacy.[[2]](#footnote-3)

## 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 will be applicable as law in the UK with effect from 25th May 2018.

# Roles of data controllers and processors

## Data controller

At Dorridge Surgery the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. He/she should be able to demonstrate compliance and is responsible for making sure data is:[[3]](#footnote-4)

* 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 controllers at Dorridge Surgery are the partners; they are responsible for ensuring that all data processors comply with this policy and the GDPR.

## 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:[[4]](#footnote-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

The last point shall not apply to processing carried out by public authorities in the performance of their tasks NB General Practices for the purpose of GDPR/DPA2018 are deemed to be public authorities

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

# Access

## Data subject’s rights

All data subjects have a right to access their data and any supplementary information held by Dorridge 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

The purpose for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them.

**Transparent information**

The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. Information can also be provided verbally providing the identity of the person is proven

The controller can refuse to provide information where the identity of the data subject is not able to be confirmed

Information requested must be provided within one month of receipt of request. If a data subject requests their information electronically, the information should be provide din same format where possible unless otherwise requested by the data subject.

If the data controller decides not to provide information requested by the data subject, the data controller must, within one month, advise the data subject accordingly and give information regarding how to complain or seek judicial remedy.

The information must be provided free of charge unless the requests are excessive or repetitive. If these circumstances arise, a fee may be charged, or the request can be refused. However, the proof of demonstrating excessiveness or repetiveness rests with the data controller.

 If there are any queries regarding confirming the identity of the data subject, the data controller has the right to seek further evidence.

**Information to be provided where personal data are collected from the data subject**

Where personal data relating to a data subject is collected from the data subject, the controller shall, at the time when this information is collected, provide the data subject with all of the following information:

* + the identity and the contact details of the data controller
	+ the contact details of the data protection officer
	+ the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
	+ the recipients or categories of recipients of the personal data, if any;
1. In addition to the information referred to above, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
	* the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
	* the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
	* the right to lodge a complaint with a supervisory authority;
	* the existence of automated decision-making, including profiling, referred to in [Article 22](https://gdpr-info.eu/art-22-gdpr/)(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. For example health risk calculators such as CHADVASC2 or Electronic Frailty assessment tool
2. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph. In General Practice, this could apply to national audit requirements such as the National Diabetes Programme. However, data is processed anonymously.

The above criteria also applies to data about a subject where that data has not been directly provided by the data subject. For example, information contained in outpatient letters which contains personal information about a data subject that they did not directly provide. The Practice does not have to provide copies of such information where the data subject already has the information

**Right of access by the data subject**

The data subject shall have the right to obtain from the data controller how information concerning the data subject is processed and in addition

* Purpose of processing
* Categories of personal data
* Who it is shared with
* Period of which the record will be stored and the criteria used to determine that period
* How to amend or delete an entry of personal data
* How to complain
* The possible sources of other data collected about the data subject
* The existence of automated decision making tools

**Right to rectification**

The data subject has the right to ask the data controller to amend or delete an entry about themselves. However, as General Practice holds data about health records, there will be times when erase is not possible. In these circumstances an addendum to the record can be made noting the data subject comments and objections. The data subject will be informed as to the action taken.

**Right to erasure (‘right to be forgotten’)**

The data subject has the right to request the erasure of personal data held by the data processor. At present, enquiries are ongoing as to how General Practice may meet this requirement subject to the current restrictions and processes of the current electronic patient system suppliers.

**Right to restriction of processing**

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

* 1. the accuracy of the personal data is contested by the data subject and so the data being contested will not be processed during the period of investigation
	2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
	3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
	4. the data subject has objected to processing pursuant to [Article 21](https://gdpr-info.eu/art-21-gdpr/)(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

**Right to data portability**

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible, for example, GP2GP on registering with another Practice

**Automated individual decision-making, including profiling**

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. For General Practice purposes, where data is used for profiling purposes such as CVD risk, any treatment in response would only be undertaken after a review of the entire patient record to ensure holistic treatment.

**Restrictions**

Data can be processed where the data controller has to safeguard national security, defence, public security, prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, the protection of judicial independence and proceedings, breaches of ethics for regulated professions. This also includes monitoring, inspection or regulatory function connected to the exercise of official authorities. For example, this would relate to CQC inspections of General Practice.

## Fees

Under the GDPR, Dorridge Surgery is not permitted to charge data subjects for providing a copy of the requested information; this must be done free of charge. That said, should a request be deemed either “unfounded, excessive or repetitive”, a reasonable fee may be charged, subject to the comments in section Transparent Information. Furthermore, a reasonable fee may be charged when requests for additional copies of the same information are made. However, this does not permit the practice to charge for all subsequent access requests.

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

## 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).

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.

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

See Appendix 3 – Application Form for Access to Health Records

## E-requests

The GDPR states that data subjects should be able to make access requests via email. Dorridge Surgery is compliant with this and data subjects can complete an e-access form and submit the form via email.

The data controller is to ensure that ID verification is requested and this should be stated in the response to the data subject upon receipt of the access request. It is the responsibility of the data controller to ensure they are satisfied that the person requesting the information is the data subject to whom the data applies.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

For Dorridge Surgery, patients are able to request on line access to their medical records for which there is a separate process for verification of identity. In the first instance, a patient requesting access to part or all of their medical record will be offered an on line GP account. Should the patient refuse this offer or not be able to identify the information required, the patient will be required to complete and submit the Application Form for Access to Health Records. The will still be required to attend the Practice in person for the identification process to be undertaken.

## 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. Requests from Third parties may be charged for.

Insurance companies will on occasion, need to access the medical condition of a patient before granting cover, this also includes solicitors acting on behalf of patients involved in claims. To enable this, the Access to Medical Reports Act 1988 gives insurance companies a clear and established legal route to access medical information. The Act also gives appropriate safeguards to patients and respects the confidential relationship between a GP and their patient. Under the Act, a GP can provide a tailored report to an insurer, with their patient’s consent, setting out only the information the insurer needs.

However, some insurance companies have instead been looking to rely on the subject access right given to consumers under the Data Protection Act in order to obtain medical records, rather than a tailored GP’s report.

A subject access request gives an individual the right to ask for all of the personal information an organisation holds about them. This is a powerful right, designed to ensure individuals can access information held about them within a specified time period and at a nominal cost. This right was not designed to underpin the commercial processes of insurers.

By making a subject access request on a patient’s behalf, an insurance company may be provided with a patient’s entire medical record, including information that is not relevant for the purpose of underwriting a policy.

Under this policy, requests for information by solicitors or insurance, or any other third party will continue to be charged for and companies will be reminded that the use of a subject data access request by the patient is not appropriate and will not be allowed.

**Security**

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

* 1. the pseudonymisation and encryption of personal data;
	2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
	3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
	4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

For Dorridge Surgery, many of the security protocols relied upon are supplied via a third party. For example, our clinical system supplier is responsible for the integrity and security of the data from the practice held on their hosted servers. The maintenance of the asset register is commissioned by BSOL to the local Commissioning Support Unit who will periodically undertake a survey of all the Practice equipment. The CSU also hold delegated responsibility for the maintenance and security of The Practice’s hardware which includes software pertaining to anti-virus protection

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Dorridge Surgery has undertaken a risk assessment of security of data and system which can be found at Appendix 4

# Data breaches

## Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.[[5]](#footnote-6) 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

Should a data breach occur, guidance will be sought from NHS Digital, who have produced a range of toolkits to assist with this process. These are as follows

 [Information Security Incident Awareness and Actions User Guide](https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/information-security-incident/user-guide)

This page also includes the Information Security Incident Good Practice Guide

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to above shall describe in clear and plain language the nature of the personal data breach

The communication to the data subject referred shall not be required if any of the following conditions are met:

* 1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
	2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to is no longer likely to materialise;
	3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

## Reporting a data breach

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](https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf).

Breaches must be reported without undue delay or within 72 hours of the breach being identified. Please also see the guidance from NHS Digital detailed above.

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
* Likely consequences of the breach
* 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](https://ico.org.uk/media/for-organisations/documents/2666/security_breach_notification_form.doc) should be used to report a breach. Failure to report a breach can result in a fine of up to €10 million.[[6]](#footnote-7)

The data controller is to ensure that all breaches at Dorridge 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

## 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 Dorridge 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

# Data erasure

## 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

## Notifying third parties about data erasure requests

Where Dorridge Surgery 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; this is so long as it is achievable and reasonably practical to do so.

This policy will be updated once the NHS IGA have issued guidance regarding data erasure.

There could be national and regional teams or processes which take data from our systems to process either in relation to direct care of the patient (for example Summary Care Records), or for audit purposes (for example the National Diabetes audit). Where possible and appropriate, data is supplied anonymised. Patients have the right to opt out of these data processes. The Practice will code their record as appropriate to prevent this process from occurring wherever possible. It is not feasible however, to notify each third party when this occurs on a patient by patient basis.

# Consent

## Appropriateness

Consent is appropriate if data processors are in a position to “offer people real choice and control over how their data is used”.[[7]](#footnote-8) 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.

## 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
* When they consented
* How they consented
* What information the data subject was told

For Dorridge Surgery, we do not always rely on consent for processing data, but on Article 9 paragraph 2 subsection h.

# Preparing for the GDPR

## 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 Dorridge 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 (including off-site storage if applicable).

Annex A details the process of data mapping at Dorridge Surgery.

## 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 Dorridge Surgery will be involved in the mapping process, thus enabling the wider gathering of accurate information.

## Data Protection Impact Assessment

The DPIA is the most efficient way for Dorridge 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. The controller shall seek the advice of the data protection officer, when carrying out a data protection impact assessment.

In accordance with [Article 35](https://gdpr-info.eu/art-35-gdpr/) 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

Prior to GDPR, the Practice already has data sharing agreements in place with various third parties. Where these exist, they have not been initiated on the part of the Practice, therefore, the responsibility for reviewing the previous impact assessment rests with the originator of the process

## 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

Annex B provides a template that is to be used to carry out a DPIA at Dorridge Surgery.

# Summary

Given the complexity of the GDPR, all staff at Dorridge Surgery must ensure they fully understand the requirements within the Regulation, which become enforceable by law with effect from 25th May 2018. Understanding the changes required will ensure that personal data at Dorridge 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 B – The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at Dorridge Surgery.

**Step 1 – Determining the need**

|  |  |  |
| --- | --- | --- |
| DOES THE PROCESS INVOLVE ANY OF THE FOLLOWING: | YES | NO |
| The collection, use or sharing of existing data subjects’ health information? |  |  |
| The collection, use or sharing of additional data subjects’ health information? |  |  |
| The use of existing health information for a new purpose? |  |  |
| The sharing of data subjects’ health information between organisations? |  |  |
| The linking or matching of data subjects’ health information which is already held? |  |  |
| The creation of a database or register which contains data subjects’ health information? |  |  |
| The sharing of data subjects’ health information for the purpose of research or studies (regardless of whether the information is anonymised)? |  |  |
| The introduction of new practice policies and protocols relating to the use of data subjects’ personal information? |  |  |
| The introduction of new technology in relation to the use of data subjects’ personal information, i.e. new IT systems, phone lines, online access, etc? |  |  |
| Any other process involving data subjects’ health information which presents a risk to their “rights and freedoms”? |  |  |

**If the answer is yes to one or more of the above questions, a DPIA is required; proceed to Step 2.**

**Step 2 – Assessing the risks**

|  |
| --- |
| **Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject** |
| What information is being collected and how? |  |
| Where is the information being collected from and why? |  |
| How often is the information being collected? |  |
| **Information use – Is the data obtained for specified, explicit and legitimate purposes?** |
| What is the purpose for using the information? |  |
| When and how will the information be processed? |  |
| Is the use of the information linked to the reason(s) for the information being collected? |  |
| **Information attributes – Personal data shall be accurate and, where necessary, kept up to date** |
| What is the process for ensuring the accuracy of data? |  |
| What are the consequences if data is inaccurate? |  |
| How will processes ensure that only extant data will be disclosed? |  |
| **Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| What security processes are in place to protect the data? |  |
| What controls are in place to safeguard only authorised access to the data? |  |
| How is data transferred; is the process safe and effective? |  |
| **Data subject access – Personal data shall be accurate and, where necessary, kept up to date** |
| What processes are in place for data subject access? |  |
| How can data subjects verify the lawfulness of the processing of data held about them? |  |
| How do data subjects request that inaccuracies are rectified? |  |
| **Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| Will information be shared outside the practice; are data subjects made aware of this? |  |
| Why will this information be shared; is this explained to data subjects? |  |
| Are there robust procedures in place for third-party requests which prevent unauthorised access? |  |
| **Retention of data – Personal data shall be 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** |
| What are the retention periods associated with the data? |  |
| What is the disposal process and how is this done in a secure manner? |  |
| Where is data stored? If data is moved off-site, what is the process; how can data security be assured? |  |

**Continued overleaf...**

**Step 3 – Risk mitigation**

|  |
| --- |
| **Information collection – The risk** |
| Personal data is collected without reason or purpose – increased risk of disclosure. |
| **Information collection – The mitigation** |
| The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected. |
| **Information use – The risk** |
| Personal data is used for reasons not explained to, or expected by, the data subjects.  |
| **Information use – The mitigation** |
| Clearly explain and display to data subjects how their information will be used.  Data-sharing requires a positive action, i.e. opting in, not opting out! |
| **Information attributes – The risk** |
| Data is inaccurate or not related to the data subject. |
| **Information attributes – The mitigation** |
| Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended. |
| **Information security – The risk** |
| Unauthorised access to data due to a lack of effective controls or lapses of security/procedure. |
| **Information security – The mitigation** |
| Ensure that staff are aware of the requirement to adhere to the practice’s security protocols and policies; conduct training to enhance current controls. |
| **Data subject access – The risk** |
| Data subjects are unable to access information held about them or to determine if it is being processed lawfully. |
| **Data subject access – The mitigation** |
| Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.  |
| **Information disclosure – The risk** |
| Redacting information before disclosure might not prevent data subjects being identified – i.e. reference to the data subject may be made within the details of a consultation or referral letter. |
| **Information disclosure – The mitigation** |
| Make sure the policy for disclosure is robust enough to ensure that identifying information is removed. |
| **Retention of data – The risk** |
| Data is retained longer than required or the correct disposal process is not adhered to. |
| **Retention of data – The mitigation** |
| Ensure that practice policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance. |

**Step 4 – Recording the DPIA**

An **example** of a DPIA report is shown overleaf. There is no stipulated format for the report; each practice can amend as they deem necessary.

**Step 5 – Reviewing the DPIA**

The review process is detailed in the report.

|  |
| --- |
| **Data Protection Impact Assessment Report** |

|  |  |
| --- | --- |
| **Practice name** | Dorridge **Surgery** |
| **Data controller** | **Practice Manager** |
| **Date of assessment** | **[Insert date]** |
| **Process assessed** | **[Referral process]** |

**Overview:**

Dorridge Surgery currently adheres to internal policies and national legislation and guidance for all processes that involve personal data. To ensure that the practice is compliant with the GPDR, which comes into effect on 25th May 2018, a review of all processes is being undertaken.

**The need:**

Having completed Step 1 of the DPIA, when asked “Does the process involve any of the following”, this question merited a “yes” response: The sharing of data subjects’ health information between organisations.

The practice is frequently required to share data subjects’ personal data – more specifically, personal details and healthcare between organisations. That is the sharing of data between Dorridge Surgery and UHB/HEFT in BSOL This is a requirement to ensure that data subjects receive the necessary care and treatment commensurate with their clinical condition(s).

**Assessing the risk:**

|  |
| --- |
| **Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject** |
| What information is being collected and how? | Personal details, healthcare information |
| Where is the information being collected from and why? | Data subjects and IT system  |
| How often is the information being collected? | During consultations, which are on an as-needed basis |
| **Information use – Is the data obtained for specified, explicit and legitimate purposes?** |
| What is the purpose for using the information? | To enable the provision of effective healthcare treatment |
| When and how will the information be processed? | Recorded during consultations onto the EMIS Web clinical system |
| Is the use of the information linked to the reason(s) for the information being collected? |  Yes |
| **Information attributes – Personal data shall be accurate and, where necessary, kept up to date** |
| What is the process for ensuring the accuracy of data? | Asking the data subject to confirm details and ensuring the correct patient record is used when recording the information |
| What are the consequences if data is inaccurate? | Incorrect patient record updated; delay in treatment and or referral; potentially adverse impact on patient health |
| How will processes ensure that only extant data will be disclosed? | Only that information which is pertinent to the referral will be used; this is extracted onto medical templates using the IT system |
| **Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| What security processes are in place to protect the data? | Only authorised users can access the data. Staff must adhere to the NHS policy for the use of IT equipment |
| What controls are in place to safeguard only authorised access to the data? | Regular audits of access to healthcare records. All users have an individual log-on and the system is password restricted |
| How is data transferred; is the process safe and effective? | The data is transferred electronically using end-to-end encryption |
| **Data subject access – Personal data shall be accurate and, where necessary, kept up to date** |
| What processes are in place for data subject access? | Data subjects can access limited information using online services or by submitting a SAR |
| How can data subjects verify the lawfulness of the processing of data held about them? | By accessing their records and viewing how information has been processed |
| How do data subjects request that inaccuracies are rectified? | Data subjects can request that information held about them be changed by asking for an appointment with the data controller |
| **Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| Will information be shared outside the practice; are data subjects made aware of this? | Yes, the practice privacy policy details this information |
| Why will this information be shared; is this explained to data subjects? | Yes, to facilitate the necessary examination and treatment of data subjects |
| Are there robust procedures in place for third-party requests which prevent unauthorised access? |  Yes, authority must be provided by the third party who also included either a written statement or consent form, signed by the data subject |
| **Retention of data – Personal data shall be 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** |
| What are the retention periods associated with the data? | GP records are retained for a period of 10 years following the death of a patient |
| What is the disposal process and how is this done in a secure manner? | At the end of the retention period the records will be reviewed and if no longer needed then destroyed |
| Where is data stored? If data is moved off-site, what is the process; how can data security be assured? | Patient data is stored electronically on the IT system (EMIS Web) and hard copies of patient records (if held) are stored in the administration office, which can only be accessed by authorised personnel |

To assess the risk of this process, this risk matrix was used:



The risk for this process has been recorded in the risk register, which details the mitigating actions taken to reduce the risk. The register is shown overleaf.



**Review requirements**

The referral process is fundamental to effective patient healthcare. The process is to be continually monitored to assess the effectiveness of the process; this can be achieved through internal audit.

This DPIA is to be reviewed when there are changes to the referral process (no matter how minor they may seem).

**Version 1 – General Data Protection Regulation Policy Version 1**

1. [NHS Digital GDPR guidance](https://www.digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance) [↑](#footnote-ref-2)
2. [EU GDPR overview](https://www.eugdpr.org/eugdpr.org.html) [↑](#footnote-ref-3)
3. [Article 5 GDPR Principles relating to processing of personal data](https://gdpr-info.eu/art-5-gdpr/) [↑](#footnote-ref-4)
4. [Article 6 Lawfulness of processing](https://gdpr-info.eu/art-6-gdpr/) [↑](#footnote-ref-5)
5. [ICO – Personal data breaches](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) [↑](#footnote-ref-6)
6. [ICO Personal data breaches](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) [↑](#footnote-ref-7)
7. [ICO Consent](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) [↑](#footnote-ref-8)