General Data Protection Regulation Policy & DPIA

Version:	Review date:	Edited by:	Approved by:	Comments:
1	24.05.2019	MJ	DAL	
2	27.05.2020	MJ	DAL	Updated DPO details

Table of contents

1 Introduction

1.1 Policy statement

The EU General Data Protection Regulation (GDPR herein) will come into force on 25th May 2018, superseding the Data Protection Act (DPA) 1998. The GDPR applies to all EU member states and The Alexandra Practice 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 contractual and therefore form part of your contract of employment. Employees will be consulted on any modifications or change to the document's status.

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 via Blue Stream Training Module GDPR. Additional support has been 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 and partners of the practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are required to use it.

2.2 Why and how it applies to them

All personnel at The Alexandra Practice 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. All staff and third party who have access to practice and patient data are classed as data processors and are subject to the requirements of the GDPR Legislation.

Definition of terms

2.3 Data Protection Officer

An expert on data privacy, working independently to ensure compliance with policies and procedure. For The Alexandra Practice, this is **Shavarnah Purves, Senior Information Governance Officer, Manchester Health and Care Commissioning ,**
0161 765 4428 | shavarnah.purves@nhs.net

Data Protection Authority

National authorities tasked with the protection of data and privacy.

2.4 Data Controller

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

2.5 Data Processor

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

2.6 Data Subject

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

2.7 Personal data

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

2.8 Processing

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

2.9 Recipient

The entity to which personal data is disclosed.

3 The build-up to the GDPR

3.1 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

3.2 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. 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]

3.3 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]

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

4 Roles of data controllers and processors

4.1 Data controller

At The Alexandra Practice the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. The Practice should be able to demonstrate compliance and is responsible for making sure data is:[3]

- 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 is The Alexandra Practice (namely the GP Partners) they are responsible for ensuring that all data processors comply with this policy and the GDPR.

4.2 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:[4]

[1] NHS Digital GDPR guidance
[2] EU GDPR overview
[3] Article 5 GDPR Principles relating to processing of personal data
[4] Article 6 Lawfulness of processing

- 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 The Alexandra Practice all staff and third parties with access to patient and practice data are classed as data processors as their individual roles will require them to access, protect and process personal data.

5 Access

5.1 Data subject's rights

All data subjects have a right to access their data and any supplementary information held by The Alexandra Practice. 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.

5.2 Fees

Under the GDPR, we are 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. 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.

5.3 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 (30 days) 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.

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

5.5 E-requests

The GDPR states that data subjects should be able to make access requests via email, The Alexandra Practice is compliant with this and data subjects can complete an e-access form and submit the form via our website or send a request to the practice 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.

5.6 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.

6 Data breaches

6.1 Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.[5] 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

6.2 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.
Breaches must be reported without undue delay or within 72 hours of the breach being identified.
Report via the IG Toolkit at: https://www.dsptoolkit.nhs.uk/Incidents/New/WhatHappened

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

[5] ICO – Personal data breaches

- 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

Breaches are reported via the IG Toolkit in line with NHS Digital procedures. If the toolkit determines the breach to require reporting to the ICO, then 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.[6]

The data controller is to ensure that all breaches at the Practice 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

6.3 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 will 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

7 Data erasure

7.1 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. This right is rarely applicable within NHS healthcare due to the lawful basis for retaining and processing data.

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

[6] ICO Personal data breaches

- 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

7.2 Notifying third parties about data erasure requests

Where a Practice 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.

8 Consent

8.1 Appropriateness

Consent is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[7] 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.

8.2 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
- When they consented
- How they consented
- What information the data subject was told

Although the NHS IGA have not issued definitive guidance on this subject, it is anticipated that consent will be detailed in depth in the NHS GDPR advice material. This policy will be updated to reflect the NHS guidance when published.

[7] ICO Consent

9 Preparing for the GDPR

9.1 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 has enabled the Practice to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping identifies 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 – not applicable at The Alexandra Practice)

Annex A details the process of data mapping at The Alexandra Practice

9.2 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 the practice have been involved in the mapping process, thus enabling the wider gathering of accurate information.

9.3 Data Protection Impact Assessment

The DPIA is the most efficient way for us to meet our 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 the Practice 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.

9.4 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

Annex A provides details of the DPIA at The Alexandra Practice.

Summary

Given the complexity of the GDPR, all staff at The Alexandra Practice 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 The Alexandra Practice 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

Stored at Shared drive P: Legacy, Information Governance – Lead SIRO, Dr A Larkin

Annex B – The Data Protection Impact Assessment

This document has been used to conduct a DPIA at The Alexandra Practice

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?	x	
The collection, use or sharing of additional data subjects' health information?		
The use of existing health information for a new purpose?	x	
The sharing of data subjects' health information between organisations?	x	
The linking or matching of data subjects' health information which is already held?	x	
The creation of a database or register which contains data subjects' health information?	x	
The sharing of data subjects' health information for the purpose of research or studies (regardless of whether the information is anonymised)?	x	

The introduction of new practice policies and protocols relating to the use of data subjects' personal information?		x
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?		x
Any other process involving data subjects' health information which presents a risk to their "rights and freedoms"?		x

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?	**Personal details , sensitive data and health information – social circumstances**
Where is the information being collected from and why?	**Data subjects and IT Systems hospital and third party healthcare providers plus safeguarding teams**
How often is the information being collected?	**During consultations which are on an as-needed basis. Each time mail / electronic information is received (daily) and via telephone call in emergency situations as they arrive**
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	**Provision of effective healthcare, treatment, diagnosis and prevention plus with patient consent for third party and private uses such as insurance forms and occupational health**
When and how will the information be processed?	**Recorded during consultations onto the EMIS Web clinical system, scanned into EMIS via Docman and entered by staff from reports and correspondence. Used to process referrals, pseudonymised research, safeguarding reports and with consent complete third party requests for information.**
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 – right to amendment if factually incorrect**
What are the consequences if data is inaccurate?	**Incorrect patient record updated; delay in treatment and or referral; potentially adverse impact on patient health-**

	impact on third party processes such as insurance claims
How will processes ensure that only extant data will be disclosed?	**Only information which is pertinent to any referral / request will be used; this is extracted onto medical templates using the IT system where available**
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 policy for the use of IT equipment –password protected use only for the pc , then the medical system plus the scanning system and the Practice email**
What controls are in place to safeguard only authorised access to the data?	**Regular audits of access to healthcare records. Application of confidentiality protocols for patients known or related to staff. All users have an individual log-on and the system is password restricted. NHS net use.**
How is data transferred; is the process safe and effective?	**The data is transferred electronically using end-to-end encryption. In the case of third party requests these are sent recorded delivery or collected in person with the verification of photo identification.**
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 SARs**
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 plus privacy policy detailing lawful basis**
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 and with their consent only to third parties such as insurance companies**
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 plus practice SARs policy including consent and proof of ID
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 returned to NHS England and retained for a set period following the death of a patient Private work and complaints data is retained for 10 years**
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 by NHS England – there is no process for disposal of medical system data (EMIS) so we archive this data in line with system restraints Private work and complaints documents are shredded via shred it**
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 - data is not moved off site**

Continued overleaf...

Step 3 – Risk mitigation

Information collection – The risk
Personal data is collected without reason or purpose – increased risk of disclosure. **No**
Information collection – The mitigation
The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected. **Yes**
Information use – The risk
Personal data is used for reasons not explained to, or expected by, the data subjects. **No**
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. **Possible**
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. **Yes**
Information security – The risk
Unauthorised access to data due to a lack of effective controls or lapses of security/procedure. **No**
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. **Yes**
Data subject access – The risk
Data subjects are unable to access information held about them or to determine if it is being processed lawfully. **Yes**
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. **Yes**
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. **Yes**
Information disclosure – The mitigation
Make sure the policy for disclosure is robust enough to ensure that identifying information is removed. **Yes**
Retention of data – The risk
Data is retained longer than required or the correct disposal process is not adhered to. **No**
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. **Yes**

Step 4 – Recording the DPIA

Our DPIA Is below

Step 5 – Reviewing the DPIA

The review process is detailed in the report.

Data Protection Impact Assessment Report	
Practice name	**The Alexandra Practice**
Data controller	**GP Partners**
Date of assessment	**25.05.2018**
Process assessed	**Treatment, referral and third party requests**

Overview:

The Alexandra Practice 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 plus others as outlined above.

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 with NHS Organisations, third party health care providers and in the cases of consent third party requestors e.g. insurance companies and other occupational health / statutory bodies. This is a requirement to ensure that data subjects receive the necessary care and treatment commensurate with their clinical condition(s) and that information is shared effectively and safely within the constraints of the law.

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 , sensitive data and health information – social circumstances**
Where is the information being collected from and why?	**Data subjects and IT Systems hospital and third party healthcare providers plus safeguarding teams**
How often is the information being collected?	**During consultations which are on an as-needed basis. Each time mail / electronic information is received (daily) and via telephone call in emergency situations as they arrive**
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	**Provision of effective healthcare, treatment, diagnosis and prevention plus with patient consent for third party and private uses such as insurance forms and occupational health**
When and how will the information be processed?	**Recorded during consultations onto the EMIS Web clinical system, scanned into EMIS via Docman and entered by staff from reports and correspondence. Used to process referrals, pseudonymised research, safeguarding reports and with consent complete third party requests for information.**
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 – right to amendment if factually incorrect**
What are the consequences if data is inaccurate?	**Incorrect patient record updated; delay in treatment and or referral; potentially adverse impact on patient health- impact on third party processes such as insurance claims**
How will processes ensure that only extant data will be disclosed?	**Only information which is pertinent to any referral / request will be used; this is extracted onto medical templates using the IT system where available**
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 policy for the use of IT equipment – password protected use only for the pc , then the medical system plus the scanning system and the Practice email**
What controls are in place to safeguard only authorised access to the data?	**Regular audits of access to healthcare records. Application of confidentiality protocols for patients known or related to staff. All users have an individual log-on and the system is password restricted. NHS net use.**
How is data transferred; is the process safe and effective?	**The data is transferred electronically using end-to-end encryption. In the case of third party requests these are sent recorded delivery or collected in person with the verification of photo identification.**
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 SARs**
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 plus privacy policy detailing lawful basis**
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	**Yes, the practice privacy policy details this information**

of this?	
Why will this information be shared; is this explained to data subjects?	**Yes, to facilitate the necessary examination and treatment of data subjects and with their consent only to third parties such as insurance companies**
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 plus practice SARs policy including consent and proof of ID**
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 returned to NHS England and retained for a set period following the death of a patient Private work and complaints data is retained for 10 years**
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 by NHS England – there is no process for disposal of medical system data (EMIS) so we archive this data in line with system restraints Private work and complaints documents are shredded via shred it**
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 - data is not moved off site**

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

Probability	Severity of Impact/Consequences			
		Minor	Moderate	Major
	Frequent	Medium	High	High
	Likely	Low	Medium	High
	Remote	Insignificant	Low	Medium

The risk for this process has been deemed as low – please refer to this risk questions proceeding the report.

Review requirements

The referral and data sharing processes outlined are fundamental to effective patient healthcare and patient requests. The process is to be continually monitored to assess the effectiveness of the process.

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

Mandatory review date: 25.05.2022

Signature: *M. Jones*

Melanie Jones
Practice Manager

25.05.2018 / Reviewed 27.05.2020 amended DP Details
Review due: 27.05.2022