Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

The Data Protection Impact Assessment

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?	X	
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.

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

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?	**Patient and employee personal information**
Where is the information being collected from and why?	**From the data subjects to comply with legal obligations**
How often is the information being collected?	**Routinely**
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	**To provide services relating to health care and to ensure statutory compliance**
When and how will the information be processed?	**As and when required**
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?	**Wherever possible, official documentation is required to ensure accuracy of data. As the information is provided voluntarily, the data is only as accurate as it is provided at the time of request.**
What are the consequences if data is inaccurate?	**Mistaken identity, incorrect health information**
How will processes ensure that only extant data will be disclosed?	**Routine information updates and regular data review**
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?	**Adequate premises security arrangements, adequate confidentiality processes and regular reviews of access**
What controls are in place to safeguard only authorised access to the data?	**Premises security, confidentiality statement forms, NHS smart card access**
How is data transferred; is the process safe and effective?	**Data is stored and transferred via secure channels provided by CCG IT and clinical system providers which ensures that data sharing agreements are in place and the providers are GDPR compliant as per NHSE guideance.**

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

Data subject access – Personal data shall be accurate and, where necessary, kept up to date	
What processes are in place for data subject access?	**Policies**
How can data subjects verify the lawfulness of the processing of data held about them?	**Privacy notice, GPDR policy**
How do data subjects request that inaccuracies are rectified?	**Via a formal request with supporting documentation.**
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?	**Patient health information is shared in guidance with statutory obligations. The Practice is a research practice and appropriate notifications are available on the website and in the waiting area.**
Why will this information be shared; is this explained to data subjects?	**The reason for sharing information is available on the website and in the waiting area. If the patient requests further information, this is provided on request.**
Are there robust procedures in place for third-party requests which prevent unauthorised access?	**Yes.**
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?	**As per the retention schedule**
What is the disposal process and how is this done in a secure manner?	**Confidential data disposal is overseen by**
Where is data stored? If data is moved off-site, what is the process; how can data security be assured?	**Data is stored on-site.** **For external backup, the data is stored on an encrypted drive and stored in a fire-proof safe.**

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

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. **Personal data collection is part of induction training as well as meetings. No personal data is collected without reason or purpose.**
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! **Patients are routinely asked at the time of registration and referrals for opting in or out of data sharing. Implied consent is in place which is constantly being updated. The practice is also on the process of conducting an explicit consent exercise following the contact detail update campaign.**
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. **Identity verification is used when confirming details, which involves confirming at least 2 data points or a proof of ID.**
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. **The practice has policies in place to ensure staff are aware of requirements, including contract, job description, mandatory training and appraisal.**
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. **There is an active campaign to update patient contact details and to advertise online services. Not**

all patients have access to the required equipment or routes, which may hinder their engagement. Online Access provision is part of all new registrations.
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. **Our GPDR policy is compliant with this requirement.**
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. **The practice has a comprehensive data retention schedule and data is disposed as part of regular review.**

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

Step 4 – Recording the DPIA

Overview:

The 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, 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 The Practice and Brent CCG and local providers. 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

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

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.

Neasden Medical Centre
21 Tanfield Avenue
London
NW2 7SA
Tel: 020 8208 0306
Fax: 020 8452 4324

Greenhill Park Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8208 0306
Fax: 020 8452 4324

St. Andrew's Medical Centre
Greenhill Park
London
NW10 9AR
Tel: 020 8459 7755
Fax: 020 8452 4324

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

Step 5 – Reviewing the DPIA

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).

Mandatory review date: 30/09/2021

Signature:

Krisztina Thaisz

Practice Manager

30/09/2020