GDPR AND CONFIDENTIALITY POLICY

DOCUMENT CONTROL

DOCUMENT REVISION AND APPROVAL HISTORY

Document name:	GDPR and Confidentiality Policy
Document Classification:	Corporate
Version:	2
Name of originator/author:	Rowonara Uddin
Target audience:	GPs, Managers and all staff
Policy Owner:	Josie Jones
Date created	6.6.2018
Date ratified:	0.06.2018
Ratified by:	The Board
Date published to Internet site:	11/04/2024
Date of Completion of Equality Impact Assessment	11/04/2024
Date of Environmental Impact Assessment (if applicable)	11/04/2024
Responsible committee:	Governance Committe
Superseded policy (if applicable):	1
Review Frequency	Every 3 years after created date.
Date of Last Review	08.08.2022
Next review date:	01/08/2025

Version	Date	Version Created By:	Version Approved By:	Comments/Changes
1	6.5.2018	Rowsonara Uddin	Rabia Begum	Reviewed by Rabia Begum 29/05/2018
	29.5.2018	Rowsonara Uddin	Governance Commitee	Reviewed and Approved
		Rowsonara Uddin	Board	Approved
2	23.1.2020	Naomi Frazer		
2	03.2.2021	Naomi Frazer		Next Review Jan 2024
2	08.08.2022	Josie Jones		Next Review Aug 2025

CONTENTS

1. Introduction

1.0	GDPR Background Following the leave of Britain from the EU, GDPR will be retained in domestic law, sitting alongside an amended version of the Data Protection Act 1998. The government has published a 'Keeling Schedule' which shows amendments. [1] The UK GDPR retains the same key principles, rights and obligations. 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 However, there are implications for the rules on transfers of personal data between the UK and the EEA.

2. Aim and Scope

2.1	**Aim** The Data Protection, GDPR and Confidentiality Policy has been developed to provide awareness and guidance to Our Health Partnership staff on the impact of the General Data Protection Regulation (GDPR) that was implemented within the European Union (EU) on 25 May 2018.
2.2	**Scope** This policy must be followed by all staff who are employed by or on behalf of OHP including those on temporary or honorary contracts, secondments, volunteers, bank/temporary/locum staff, Board members, students and any staff working on an individual contractor basis or who are employees for an organization contracted to provide services to OHP

3. Definitions of terms

3.1	**Data Protection Bill** The Data Protection Act 2018 sets out the data protection framework in the UK, alongside the GDPR. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies in the UK – for example by providing exemptions. It also sets out the separate data protection rules for law

[1] Keeling Schedule

	enforcement authorities, extends data protection to some other areas such as national security and defense, and sets out the Information Commissioner's functions and powers.
3.2	**Data Protection Officer** An expert on data privacy, working independently to ensure compliance with policies and procedure.
3.3	**Data Protection Authority** National authorities tasked with the protection of data and privacy.
3.4	**Data Controller** The entity that determines the purposes, conditions and means of the processing of personal data
3.5	**Data Processor** The entity that processes data on behalf of the Data Controller.
3.6	**Data Subject** A natural person whose personal data is processed by a controller or processor.
3.7	**Personal data** **The GDPR defines personal data as:** • Relating to a living human being who can be directly or indirectly identified • Identifiers include but are not limited to: - Name - Date of Birth - Postcode - Address - National Insurance Number - Photographs, digital images etc - NHS number - Hospital Number - Date of Death - Passport Number - Online identifiers and location data
3.8	**Definition of Special Categories Data** Special category data requires additional safeguards when being shared or disclosed in line with guidance and legislation. This includes but is not limited to: • Data concerning health, sex life or sexual orientation • Racial or ethnic origins • Trade union membership • Political opinions • Religious or philosophical beliefs • Genetic/biometric data (fingerprints, facial recognition etc)

	PROCESSING Any operation performed on personal data, whether automated or not.
3.9	**Recipient** The entity to which personal data is disclosed.

4. Roles of data controllers and processors

4.1	Data controller At [insert practice name] 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:[2] • 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 [insert practice name] as the data controller is 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:[3] • The data subject has given consent to the processing of his/her personal data for one or more specific purposes

[2] Article 5 GDPR Principles relating to processing of personal data

[3] Article 6 Lawfulness of processing

	• 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 [insert practice name], all staff are classed as data processors as their individual roles will require them to access 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 [insert practice name]. 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 [Insert practice name] ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations: • Waiting room/ reception • Practice website • Practice information leaflet • [Add any additional areas here] To comply with the GDPR, all practice privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the GDPR. The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them.

5.2	Fees Under the GDPR, [insert practice name] 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. 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 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. [Insert practice name] 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
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. GDPR and Brexit

6.0	Transfer restrictions will be delayed for at least four months, following the end of the transition period on 31 December 2020. For up-to-date guidance, please refer to https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/about-this-guidance/

7. Data breaches

7.1	**Data breach definition** A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.[4] Examples of data breaches include: • Unauthorised third-party access to data • Loss of personal data • Amending personal data without data subject authorisation • The loss or theft of IT equipment which contains personal data • Personal data being sent to the incorrect recipient
7.2	Reporting a data breach Where a practice wishes to seek advice then they must do so via their DPO in the first instance. The DPO will endeavor to provide the relevant advice and contact an external call off (if necessary). Only under exceptional circumstances can a practice bypass this step and seek advice directly from an external body. Any breach that is likely to have an adverse effect on an individual's rights or freedoms must be reported. The Practice must log the breach via the DSP toolkit, which then decides whether the breach meets minimum requirements to be escalated to the ICO. Breaches must be reported without undue delay or within 72 hours of the breach being identified. When a breach is identified and it is necessary to report the breach, the report is to contain the following information: • Organisation details • Details of the data protection breach

[4] ICO – Personal data breaches

	• 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 Failure to report a breach can result in a fine of up to €10 million.[5] The data controller is to ensure that all breaches at [insert practice name] 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. Our Health Partnership recommends this be recorded as a significant event in Team Net.
7.3	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 record the incident on the DSP toolkit. 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 [insert practice name] 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.

8. Data breaches

8.1	### Erasure Data erasure is also known as the "right to be forgotten", which enables a data subject to request the deletion of personal data where there is no compelling reason to retain or continue to process this information. It should be noted that the right to be forgotten does not provide an absolute right to be forgotten; a data subject has a right to have data erased in certain situations. The following are examples of specific circumstances for data erasure:

[5] ICO Personal data breaches

	• 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
8.2	Where [insert practice name] 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.

9. Consent

9.1	**Appropriateness** Consent is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[6] The GDPR states that consent must be unambiguous and requires a positive action to "opt in", and it must be freely given. Data subjects have the right to withdraw consent at any time.
9.2	Obtaining consent If it is deemed appropriate to obtain consent, the following must be explained to the data subject: • Why the practice wants the data. • How the data will be used by the practice • The names of any third-party controllers with whom the data will be shared. • Their right to withdraw consent at any time. All requests for consent are to be recorded, with the record showing: • The details of the data subject consenting • When they consented • How they consented • What information the data subject was told

[6] ICO Consent

	Consent is to be clearly identifiable and separate from other comments entered into the healthcare record. At [insert practice name] it is the responsibility of the data controller [insert name / role] to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (patients) are fully aware of their right to withdraw consent and must facilitate withdrawal as and when it is requested.
9.3	**Parental consent** Whilst the GDPR states that parental consent is required for a child under the age of 16, the DPA18 will reduce this age to 13 in the UK. Additionally, the principle of Gillick competence remains unaffected; nor is parental consent necessary when a child is receiving counselling or preventative care.

10 GDPR Requirements

10.1	**Data mapping** Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable [insert practice name] to undertake a thorough assessment of the risks associated with current data processes. It is a requirement for the DSP toolkit. 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 [insert practice name].
10.2	**Data mapping and the Data Protection Impact Assessment** Data mapping is linked to the Data Protection Impact Assessment (DPIA), and when the risk analysis element of the DPIA process is undertaken, the information ascertained during the mapping process can be used. Data mapping is not a one-person task; all staff at [insert practice name] will be involved in the mapping process, thus enabling the wider gathering of accurate information.
10.3	**Data Protection Impact Assessment** The DPIA is the most efficient way for [insert practice name] to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs. In accordance with Article 35 of the GDPR, DPIA should be undertaken where:

	• A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; then the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. • Extensive processing activities are undertaken, including large-scale processing of personal and/or special data DPIAs are to include the following: • A description of the process, including the purpose • An evaluation of the need for the processing in relation to the purpose • An assessment of the associated risks to the data subjects • Existing measures to mitigate and control the risk(s) • Evidence of compliance in relation to risk control It is considered best practice to undertake DPIAs for existing processing procedures to ensure that [insert practice name] 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. For any new processes affecting all OHP practices, OHP central will provide a DPIA. For transparency, DPIAs should be published for patients to view.
10.4	**DPIA process** The DPIA process is formed of the following key stages: • Determining the need • Assessing the risks associated with the process • Identifying potential risks and feasible options to reduce the risk(s) • Recording the DPIA • Maintaining compliance and undertaking regular reviews Annex B provides a template that is to be used to carry out a DPIA at [insert practice name].
10.5	**Privacy Notices** A privacy notice should inform individuals on how their data may be used and who it is shared with. Under the GDPR, organisations are required to provide the following information in their privacy notice: • Contact details of the organization • Contact details for the data protection officer

	• Who data will be shared with, including any information that may need to be shared with other professional bodies either in the UK or across countries • How long data will be stored for • The individual's right to have personal data deleted, or rectified in certain circumstances • The individual's right to make a subject access request • Any information provided to individuals must be clear, concise, transparent and easily accessible. Privacy notices should be prominently displayed via a number of methods by each practice.
10.6	**Data Security and Protection (DSP) Toolkit** The DSP toolkit is an online self-assessment tool for data security which allows organizations to measure their performance against the National Data Guardian's 10 data security standards and hence supports organizations in demonstrating GDPR. Each OHP practice is expected to complete the DSP Toolkit on an annual basis.

11 Data Protection Principles

11.0	### Data protection, quality and security As members of OHP, all practices will be expected to adhere to a high standard of data protection and continue to review their processes in light of new risks and breaches. Technical and organisational measures should be implemented by OHP practices. For example. - Restricting access to paper records via lockable room or door, and risk assessment of any cleaning staff requiring access to this room - Use of smartcards - Locking of PCs/rooms when not in use - Not leaving personal identifiable data on view/in printer/on desk/in vehicles etc - Check of identity before releasing data for a Subject Access Request, third party request, or providing a virtual consultation - Having robust Data Sharing Agreements in place - Ensure staff have signed confidentiality agreements - Role based access - Encryption of emails containing patient identifiable data - Ensuring any personal devices being used for homeworking is password protected, not used by others, has spyware/malware software and a firewall in place - Regular audits of access to IT systems - Not use public WiFi to access

	Practices will ensure patient records are accurate and kept up to date, regularly checking contact details with the patients, and providing online record access where appropriate. Patient records will be retained in line with the Records Management Code of Practice for Health and Social Care 2016[7] and for any other records helds will comply with statutory retention periods. Network security of practice IT systems will be maintained by the commissioned IT service.

12 National Data opt Out.

12.1	**What is the national data opt out?** The national data opt out allows patients to opt out of all sharing of their identifiable data for purposes not related to direct patient care (such as research or planning). There are a number of exceptions: • Sharing to protect public health – diagnosis of communicable diseases, prevent/control their spread, deliver and monitor vaccination problems • Sharing for a legal requirement[8] • Sharing in relation to public interest (e.g. reporting of gun/knife wounds, patient's fitness to drive and reporting concerns to DVLA)[9]
12.2	**Compliance** Practice clinical systems provide reporting and search modules, enabling you to remove records of patients who have registered a national data opt-out from any data disclosures you have identified as being in scope. Practices should update processes for handling new disclosure requests, to ensure the national data opt out policy is considered before data disclosures take place. Patients and staff should be made aware of the national data opt-out and how the practice will comply. Practices should update their privacy notice and website to reflect the national opt out.[10] Text to be included can be found in Annex C.

[7] Records Management Code of Practice for Health and Social Care 2016

[8] https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/legally-required-data-disclosures

[9] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga

13 Roles and Responsibilities.

13.1	**Data Protection Officer** All organisations whose core activities involve the processing of 'special category' or sensitive personal data, such as GP practices, need to appoint a DPO. The role of the DPO is defined under article 39 of the regulations: • Informing and advising the organization and its employees of their data protection obligations under the GDPR • Monitoring the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits • Serving as the contact point to the data protection authorities for all data protection issues, including data breach reporting • Advising on the necessity of data protection impact assessments (DPIAs) and the manner of their implementation and outcomes The Our Health Partnership DPO is required to act independently in the way they carry out their duties.
13.2	**All staff** All staff at Our Health Partnership are responsible for data security and therefore must understand and comply with this policy and associated guidance. In particular all staff should undertake their mandatory annual Data Security Awareness training and understand: • What information they are using, how it should be protectively handled, stored and transferred • What procedures, standards and protocols exist for the sharing of information with others • How to report a suspected breach of information security • Their responsibility for raising any information security concerns with the Data Protection Officer
13.3	**Training and support** Training is available via a number of platforms such as e-Learning for Health, to provide guidance and support, to help those to whom it applies understand their rights and responsibilities under this policy. Additional support can be provided to managers and supervisors by Our Health Partnership to enable them to deal more effectively with matters arising from this policy.

14 Summary

14.0	Given the complexity of the GDPR, all staff at [insert practice name] must ensure they fully understand the requirements within the Regulation, which became enforceable by law with effect from 25th May 2018. Understanding the changes required will

	ensure that personal data at [insert practice name] 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 Protection Impact Assessment

This document is to be used to conduct a DPIA at [insert practice name].

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	**[Insert practice name]**
Data controller	**[Insert name of controller]**
Date of assessment	**[Insert date]**
Process assessed	**[Referral process]**

Overview:

[Insert practice name] 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 [insert practice name] and [NHS Hospital Trusts] in [state area]. 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:

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 recorded in the risk register, which details the mitigating actions taken to reduce the risk. The register is shown overleaf.

REF #	DATE	RISK	RISK SCORE			OWNER	MITIGATING ACTION(S)	SCORE POST ACTION(S)			PROGRESS	STATUS	DATE CLOSED
			Probability	Impact	Status			Probability	Impact	Status			
PI01/18	01/02/18	Data subjects are unaware that their data is being shared with other organisations i.e. hospitals	Likely	Major		I N Pain (PM)	PM to produce statement for website, poster for waiting room explaining the need to share data. Draft and implement a policy for positive opt-in actions for data sharing.	Likely	Minor		Statement written and uploaded. Waiting Rm poster in progress. Policy drafted pending approval.	Ongoing	

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: [insert review date]

Signature:

[Insert name]

[Position]

[Date]

[Version] – [i.e. Version 1.0 – Reviser – I N Pain – Document Created]

Annex B – GDPR checklist

This checklist has been designed to support practice managers in preparing for the GDPR.

Creating a culture of awareness	
All staff need to be aware that the GDPR becomes applicable by law in the UK with effect from the 25th May 2018. • It is essential that they understand the impact this will have on them in their roles. • Have you shared the practice GDPR policy with them or signposted them to further information, i.e. ico.org.uk or NHS Digital IGA?	
Action complete (✓ or ✗)	

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

Data Protection Impact Assessment (DPIA)	
The DPIA is the most efficient way for the practice to meet their data protection obligations. DPIAs are mandatory in accordance with Article 35 of the GDPR and should be undertaken when: • A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations which present similar high risks • Extensive processing activities are undertaken, including large-scale processing of personal and/or special data Have DPIAs been completed? Best practice is to undertake DPIAs for existing processes to ensure that data protection obligations are met. Once you have conducted a data mapping exercise and started your information register. OHP DPO will come to the Practice to assist you with DPIA for existing procedures. You are welcome to use the DPIA example on page 26.	
Action complete (✓ or ✗)	

Continued overleaf…

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

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

Subject access requests	
All data subjects have a right to access their data and any supplementary information held. Does the practice policy reflect the changes and do staff understand: • The changes affecting subject access requests? • There is no fee applicable as of 25th May 18? • The response time is one calendar month? • Requests can be refused, but must be fully justified? • Requests can be received by email?	
Action complete (✓ or ✗)	

Processing personal data
Do data processors within the practice understand that they are responsible for the processing of data on behalf of the data controller? Do all processors know that one of the following must apply: • The data subject has given consent to the processing of his/her personal data for one or more specific purposes • Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the 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

Action complete (✓ or ✗)	

Consent
Consent is an area that has seen significant change as a result of the GDPR. • Do current processes for obtaining consent reflect the GDPR? • Do staff know that they must explain to data subjects: 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 • Are staff aware that the Data Protection Bill (DPA18) will state that parental consent is required for a child under the age of 13; Gillick competence remains unaffected
Action complete (✓ or ✗)

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

Annex C – National Data Opt Out Privacy Notice Text

The following is a recommended set of text to reference the wider use of a patient's health and care data by local and national NHS and care organisations that can be added to an organisation's website alongside the organisation's Privacy Notice. It is intended to provide a simple easy to understand message about the wider uses of data, drawing upon the language used in other materials which has been tested with patients and the public. The intention of the Template Transparency Statement is to point patients to the national online resources that have been created to support this communication to patients, and to ensure they are aware that they have a choice about the use of confidential patient information about them being used for purposes beyond their individual care.

This is not intended to replace the organisation's own Privacy Notice which needs to be specific to the organisation.

Organisations are reminded that they need to update their Privacy Notices (or 'Fair Processing' material) to satisfy the General Data Protection Regulation (GDPR) and data protection legislation. The key points to note are that the GDPR strengthens the requirements on organisations as data controllers to provide clear and concise information to patients in order to be fairly and lawfully processing information, being clear about what data is collected and how it is processed. This information should be described accurately and clearly within the organisation's Privacy Notice along with the identity and contact details of the data controller and made available to patients. Further information and guidance about Privacy Notices under GDPR is available from the Information Commissioner's Office (ICO) at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/.

Recommended text for transparency statement to be added alongside the organisation's Privacy Notice.

"How the NHS and care services use your information

([insert organisation] is one of many organisations working in the health and care system to improve care for patients and the public)[11].

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

[11] This paragraph to be inserted by national organisations such as ALBs

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and

https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

Health and care organisations have until 2020 to put systems and processes in place so they can be compliant with the national data opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care. Our organisation 'is / is not currently' compliant with the national data opt-out policy.[12] "

[12] It is recommended that this is included to be clear to patients whether your own organisation is currently compliant with the policy for applying national data opt-outs.

APPENDIX 2

EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment (EQIA) Form (Please complete all sections)			
Q1. Date of Assessment: **April 2024**		Review Date: **April 2027**	
Q2. For the policy and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups experience? i.e. are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening etc?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality?
The area of policy or its implementation being assessed:			
Race and Ethnicity	No	N/A	N/A
Gender	No	N/A	N/A
Age	No	N/A	N/A
Religion	No	N/A	N/A
Disability	No	N/A	N/A
Sexuality	No	N/A	N/A
Pregnancy and Maternity	No	N/A	N/A
Gender Reassignment	No	N/A	N/A
Marriage and Civil Partnership	No	N/A	N/A
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	No	N/A	N/A
Area of service/strategy/function			
Q3. What consultation with protected characteristic groups including patient groups have you carried out? **N/A**			
Q4. What data or information did you use in support of this EQIA? **N/A**			
Q.5 As far as you are aware are there any Human Rights issues be considered such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? **N/A**			

Q.6 What future actions needed to be undertaken to meet the needs and overcome barriers of the groups identified or to create confidence that the policy and its implementation is not discriminating against any groups			
What?	By whom	By when	Resources required

APPENDIX 3
ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact of policies, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	**Environmental Risk/Impacts to consider**	**Action Taken (where necessary)**
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	N/A
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released (e.g. lubricants, liquid chemicals)? • Does the policy fail to consider the need to provide adequate containment for these substances? (e.g. bunded containers, etc.)?	N/A
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities)? • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water)? • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	N/A
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (e.g. use a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.)? • Does the policy fail to include a procedure to mitigate the effects?	N/A

	• Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	
Energy	• Does the policy result in an increase in energy consumption levels in the Organisation? (estimate quantities)	N/A
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	N/A

APPENDIX 4
HERE FOR YOU ASSESSMENT

Our Health Partnership – We are ***'Here For You'*** Our Policy and Procedure Compliance Toolkit are service standards we have developed together. They can help us to be more consistent in what we do and say to help people to feel cared for, safe and confident in their treatment. The standards apply to how we behave not only with patients and visitors, but with all our colleagues too. They apply to all of us, every day, in everything that we do. Therefore, their inclusion in our Policies and Procedures is essential to enable us to embed them in our organization and make them a part of our everyday ethos.

Values *Please rate each value from 1 – 3* (**1 being not at all, 2 being affected and 3 being very affected**)	Score
1. Polite and Respectful: Whatever our role we are polite, welcoming and positive in the face of adversity, and are always respectful of people's individuality, privacy and dignity.	**1**
2. Communicate and Listen: We take the time to listen, asking open questions, to hear what people say; and keep people informed of what's happening.	**1**
3. Helpful and Kind: All of us keep our 'eyes open' for (and don't 'avoid') people who need help; we take ownership of delivering the help and we can be relied on.	**1**
4. Vigilant: Every one of us is vigilant across all aspects of safety, practices hand hygiene & demonstrates attention to detail for a clean and tidy environment everywhere.	**1**
5. On Stage (patients feel safe): We imagine anywhere that patients could see or hear us as a 'stage'. Whenever we are 'on stage' we look and behave professionally, acting as an ambassador for OHP, so patients, families and carers feel safe, and are never unduly worried.	**1**
6. Speak Up: We are confident to speak up if colleagues don't meet these standards, we are appreciative when they do, and are open to 'positive challenge' by colleagues	**1**
7. Informative:	**1**

We involve people as partners, helping them to be clear about their choices and how they might feel. We answer their questions without jargon. We do the same when delivering services to each other.	
8. Timely: We appreciate that other people's time is valuable, and offer a responsive service, to keep waiting to a minimum whilst ensuring we have undertaken an appropriate time and sufficient care to complete the task.	**1**
9. Compassionate: We understand the importance of body language and deliverance of tone when dealing with a variety of situations, especially those that maybe sensitive or complex. We are considerate of other people feelings, showing empathy, compassion and offering reassurance when required, whilst still adhering to deliver service	**1**
10. Accountable: Take responsibility for our own actions and results	**1**
11. Best Use of Time and Resources: Simplify processes and eliminate waste, while improving quality	**1**