THE WESTERHAM PRACTICE

Name of Policy	Data Protection Impact Assessment (DPIA) Procedure
Date of Issue	November 2020
Next Review Date	November 2021
Created By	Kent and Medway CCG GP DPO Team
For implementation By	The Westerham Practice

Contents

1 Introduction 2

2 Scope 2

3 Principles 2

4 Equality Statement 3

5 Roles and Responsibilities 3

6 The Process 4

7 Training and Support 6

8 Audit and Monitoring Criteria 7

9 Implementation and Dissemination 7

10 References 7

APPENDIX A - Screening questions 8

APPENDIX B - Full DPIA 9

APPENDIX C - Short DPIA 13

1 Introduction

1.1 The General Data Protection Regulation (GDPR) introduced a new obligation upon organisations to conduct a Data Protection Impact Assessment (DPIA) before carrying out types of processing that are likely to result in high risk to individuals' rights. This procedure details how The Westerham Practice will achieve this requirement.

1.2 Projects that involve personal or special category information (including pseudonymised data) or new technologies to process personal data give rise to privacy issue and concerns. Privacy includes 'confidentiality' and 'consent' as an overarching principle. This procedure advocates that respect for privacy and dignity must be considered at the outset of any project. To enable organisations to address any privacy concerns and risks, a technique referred to as a DPIA endorsed by the Information Commissioner's Office (ICO) must be used.

1.3 Data protection by design' is also endorsed by the Data Security and Protection Toolkit to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent and where feasible allows individuals to monitor what is being done with their data. Together the procedure enables an organisation to improve data protection and security of personal information. New Systems or processes should not 'go live' until the 'data protection by design' work has been completed.

2 Scope

2.1 This procedure applies to those members of staff that are directly employed by the practice and for whom the Practice has legal responsibility, as well as any Processors/contractors/sub-contractors/third parties processing Practice data or accessing systems, or anyone authorised to undertake work on behalf of the Practice. For those staff covered by a letter of authority/honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for or on behalf of the Practice.

2.2 This procedure provides guidance to staff and provides assurances to individual's data whose personal data is being processed, and covers all aspects of information within the organisation, including (list is not exhaustive):

- Patient/client/service user information
- Employee personal information
- Corporate information
- Commercially sensitive information

3 Principles

3.1 Data Protection by Design and Default gives personal information the same importance in business cases and planning as finance, human resources and capital and physical assets. Information governance can sometime come across as a barrier because data protection and privacy considerations have not been built in from the design of a project.

3.2 To ensure IG doesn't become a barrier, the Practice has data protection and individuals' privacy built into its business approval and procurement processes ensuring that any concerns are addressed in the early stages of procuring or commissioning any new system, service, product or process. This method guarantees that appropriate technical and organisational

measures to implement the data protection principles and safeguard individual rights are in place prior to mobilisation. This involves but is not limited to:

- Only using Processors that provide sufficient guarantees of their technical and organisational measures for data protection by design;
- Anticipating risks and privacy-invasive events before they occur, and taking steps to prevent harm to individuals;
- Making data protection an essential component of the core functionality of our processing systems and services.

3.3 **Important**: If a DPIA identifies a high risk that is unable to be mitigated, the Practice must consult the ICO before the project can go ahead.

4 Equality Statement

The Practice is committed to a policy of equality in all its employment practices in accordance with the Equality Act and principles and strives to eliminate unfair discrimination, harassment, bullying and victimisation. The practice will not unlawfully, unfairly or unreasonably discriminate or treat individuals less favourably on the grounds of gender or gender reassignment, marriage or civil partnership, pregnancy or maternity, sexual orientation, religion or belief, disability, age, race, nationality or ethnic origin.

5 Roles and Responsibilities

5.1 Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 The Practice lead for Information Governance will provide advice and guidance to all staff on all elements of Information Governance and Data Security (IG/DS). They are responsible for:

- providing advice and guidance on IG/DS to all staff;
- ensuring the consistency of IG/DS across the organisation;
- developing IG/DS policies, procedures, strategies and guidance;
- establishing protocols on how information is to be shared;
- developing IG/DS awareness and training programmes;
- ensuring compliance with Data Protection, and other information security related legislation;
- handling and responding to Freedom of Information requests; and
- implementing system wide IG/DS guidance and policy, taking into account national guidance, for example from NHS England, and the Department of Health, as well as legislative and regulatory changes.

5.3 **The Kent and Medway GP Data Protection Officers (DPO) as** employed by the CCG. The DPO is responsible for Data Protection compliance within The Westerham Practice and ‘reviews’ all DPIAs for recommendation of endorsement to the SIRO. The DPO can provide advice on:

- whether a DPIA is required;
- how the DPIA should be conducted;
- what measures and safeguards can be taken to mitigate risks;
- whether the DPIA has been carried out correctly; and
- the outcome of the DPIA and whether the processing can go ahead.

The DPO's advice to Project Managers is recorded on the final version of the DPIA. If you do not follow the DPO's advice, you should record your reasons for not doing so, ensuring that you are able to justify your decision and inform the DPO.

The DPO also monitors updates from the project managers regarding the ongoing performance of the DPIA, including how well the planned actions have been implemented to address the risks.

5.4 The Practice Manager will take responsibility for ensuring that the Practice's 'data flow map' is updated for their Practice following the completion of a DPIA where applicable.

5.5 All staff - employed by the practice must follow the requirements of this procedure and associated policies, particularly those relating to processing of patients' Information. All health professionals must also meet their own professional codes of conduct in relation to confidentiality. Where breaches of confidentiality, security alerts etc. are identified relating to an information system, a DPIA must be undertaken to provide assurance that information risk is being managed.

6 The Process

5.1 A DPIA must be completed at an early stage of the project or planned modification to an existing process or information asset. Completion of a DPIA Screening Checklist; see Appendix A, during the initial scoping phase of a Project, will establish whether your Project is likely to require a Full Scale DPIA; see Appendix B.

5.2 In response to Covid 19 a short form DPIA was developed; see Appendix C. Please note this should only be used when the practice is required to complete work required for a limited time whilst the business continuity event takes place such as during the COVID pandemic.

5.3 Stage One – Identify the need

A DPIA is not needed for every project, however to determine whether one is needed you need to answer a set of screening questions; see Appendix A. The key times when a DPIA is likely to be needed is on projects where:

The ICO advise you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any new project involving the use of personal data.

This screening process assesses the threshold and determines whether a full DPIA is needed. The decision not to proceed to a full DPIA must be recorded and stored with the relevant project documentation within the practice. As the Practices are data controllers in their own rights the Kent and Medway CCG DPO's will advise however the final decision will fall with the practices.

5.4 **Stage Two – Background, Assessment and Data Flow Capture**

If the screening questions indicate that a full DPIA is needed, proceed to stage two, which captures details of the personal information the project will process and is divided into 3 sections in the DPIA. The template is set out in Appendix B.

At this time the Project lead should also confirm that:

- ensure that relevant contracts can be reviewed if required by the practice IG leads;
- All data flows must be captured. This process identifies how we obtain information, where we store it, and who may access it.

5.5 **Stage Three – Establish the need for the data processing and its basis in law**

Establish the purposes for which the data is to be used and the basis for this in law, against the GDPR and other legislation or regulations if appropriate.

- Assess whether all the data that is recorded will be adequate for the purposes it is being used and relevant to these purposes and record this.
- Assess whether the data that is recorded will be proportionate to the purposes for which it is being used and record this.

All of this information is included in the templates.

5.6 **Stage Four – Identify Privacy and related risks**

Record the risks to individuals, including possible intrusions on privacy where appropriate.

Assess the risks to individuals against each possible risks including, but not limited to:

i) illegitimate access to data;
ii) unauthorised modification of data; and
iii) loss of data.

- Identify the specific threats which could possibly lead to each risk and the likelihood of these occurring.
- Assess the corporate risks, including regulatory action, reputational and financial damage, and loss of public trust.
- With the help of the practice IG lead and the Kent and Medway CCG DPO function, conduct a compliance check against the GDPR and other relevant legislation such as the Data Protection Act 2018.
- The practice will keep a record of the identified risks

5.7 **Stage Five – Identify and evaluate privacy solutions**

Explain how you could address and overcome each risk:

- Some might be eliminated altogether, other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.
- Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

5.8 **HIGH RISK - Stage six – Consult the ICO**

If you have identified a high risk and no measures can be taken to reduce the risk, you must consult the ICO.

- This is completed by the DPO.
- No further steps must be taken until you have received a response from the ICO.

5.9 **Stage seven – Sign off the outcomes**

Once all of the paperwork has been completed the Information Governance lead will review along with the SIRO and Caldicott Guardian for the practice will review and the Kent and Medway CCG DPO team will provide independent advice. The outcome will be recorded.

5.10 **Stage eight – Integrate the outcome back into the project**

The DPIA findings and actions should be integrated within the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation. Larger projects are more likely to benefit from a more formal review process.

A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored. The ownership of this element falls to the IAO for the project as it becomes "business-as-usual".

6 Training and Support

The Kent and Medway GP DPO team is available to offer support and guidance to Project Managers and Information Asset Owners in completing DPIAs. The practice will periodically

provide DPIA Training Workshops for staff whose roles involve project management, the objectives of the training provision are:

- To improve staff knowledge of the importance of DPIAs;
- To provide an opportunity for staff to develop skills in completing Data Flow Maps and full scale DPIAs;
- To provide an opportunity for staff to ask questions on DPIA;
- To improve understanding and confidence in completing DPIA in the future;
- To improve the practices DPIA process'.

7 Audit and Monitoring Criteria

The Practice will continually review and monitor how its Information Assets are being handled.

This procedure will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

Compliance with this procedure is monitored:

- Annually as part of the Practice's reporting on its compliance with the standards of the NHS DSP Toolkit.

Failure to adhere to the procedure may lead to an investigation of data protection regulations compliance and potential fines of up to £17.5 million for the Practice.

8 Implementation and Dissemination

Published on teamnet (practice intranet). Annual policy review document sent for all employees to review and sign.

9 References

This following statutory and national guidance has been used to develop this document:

- Data Protection Act 2018
- Data Protection Impact Assessments (ICO Website)
- Data Protection Impact Assessments (DPIA) (ICO Guidance)
- Guide to the General Data Protection Regulation (ICO Guidance)
- Data Sharing Code of Practice (ICO Guidance)

This procedure meets the requirements of the National Data Guardian's Data Security Standard 1; Assertion 1.6 of NHS Digital Data Security and Protection Toolkit, i.e. 'The use of personal information is subject to data protection by design and by default'.

THE WESTERHAM PRACTICE

APPENDIX A - Screening questions

Data Protection impact assessment (DPIA) screening questions				
Name and short description of project and data sets to be used:				
Will this project lead to:	**Yes**	**No**	**Unsure**	**Comments**
Will the project compel individuals to provide information about themselves				
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?				
Will the project result in you making decisions about individuals in ways which may have a significant impact on them?				
Will the project require you to contact individuals in ways which they may find intrusive?				
Does the project involve multiple organisations?				
Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual in a database?				
The use of special category, criminal offence data on a large scale or in a new way				
Will this profile individuals on a large scale such as tracking individuals' location or behaviour				
Will this process biometric data; process genetic data				
Will this match data or combine datasets from different sources or collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')				
Will this profile children or target marketing or online services at them				
Will this process data that might endanger the individual's physical health or safety in the event of a security breach				
Does this project use new technologies or AI				
Will this lead to systematically monitoring of publicly accessible places on a large scale (i.e. CCTV)				
Will this project result in the profiling of special category data to decide on access to services				
Will information about individuals be disclosed to organisations or people who have not previously had routine access to it?				

Name and contact details of Project lead:	
Date:	
IG log reference:	
Name of reviewer in IG:	
Comments:	
Date returned to Project lead:	

Please return to: Practice Manager

THE WESTERHAM PRACTICE

APPENDIX B - Full DPIA

Date of Assessment		Date of next Assessment	
Name of Assessment Owner *(IG Lead):*		Name of DPO	
Name of Process/Service			
List of organisations/partners involved in sharing or processing.	Controller	Processor	

Purpose of process/Service	*In here describe the proposed project in its entirety(remember you are describing this to someone who knows nothing about this project who needs to know everything)* *Give as much detail as you can. The reason behind the project, Who is involved? What technology if any is involved? How much data is involved Provide benefits of project. If it is about staff accessing data describe what staff, clinical or Admin or both.*	
Has an initial screening indicate the need for a full DPIA?	Choose an item.	
<u>Environmental Scan</u> **Consultation/checks that have been carried out regarding this process/service of similar nature, whether conducted within your organisation or by other organisations.** *Please provide any supporting documents if available*	*If you know that this project is working elsewhere describe it in here*	
Type of Data being processed	Personal Data (or embed doc list)	Sensitive Personal Data (or embed doc list)
What is the legal basis for processing of the data? **Note:** If consent lawful basis is adopted, state how consent will be obtained.	**Direct Care**. (*this is usually the case within the NHS) you will need to state if different)* Within the General Data Protection Regulation (GDPR), Article 6 sets out the conditions for lawfully processing personal data and Article 9 sets out further conditions for processing special categories of personal data. As personal data concerning health is one of the special categories, organisations that process such data must be able to demonstrate they	

	have met a condition in both Article 6 and Article 9. Under the GDPR, for processing personal data in the delivery of direct care, and for providers' administrative purposes, the most appropriate Article 6 condition that is available to all public funded health and social care organisations is Article 6(1)(e): "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 Data Controller". For work undertaken the relevant condition to rely on under Article 9 is (2)(h): "processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, provision of health or social care treatment." (read with Schedule 1 paragraph 2 of the Data Protection Act). There is an obligation in s. 251B of the Health and Social Care Act 2012 to share information amongst relevant commissioners and providers for the purposes of direct care.
Is the **National Opt out** (patients' consent) applicable to this process/service	*National data opt out is where patients can opt out of their personal identifiable data being used for another purpose that is not for 'individual care'*

Origin of the data: E.g. Patients, Practice's IT system, Publicly available	*Where is this data coming from*
Where is the data being processed/ stored? E.g. UK, Europe, USA, Other (must be limited to UK per NHS requirements)	*State where this data will be stored*
Who is impacted by the processing? E.g. Patients, employee, supplier, member of the public?	*Who will this processing affect?*
How will the data be shared? Electronically (IT system), paper or both?	*State how this data is shared*
How will the data be deleted?	*This will depend on how this data is stored and why*

Describe the process workflow	*Give a description of how the process will work from your organisations perspective.*

Has the service/process been incorporated into the data flow map?	Yes/No *This flow of data will have to be recorded in your register of processing activities – ROPA (formally known as 'data flow mapping')*
Have individuals been informed of this use of their data?	*Describe how individuals will be informed*
Are there arrangements in place for recognising and responding to SARs?	*Do staff know when a patient is requesting a copy of their own information and do they know who to give this to within your organisation?*
What measures are currently in place to protect the data subject and their rights?	*State what you have in place to allow patients to exercise their rights*
Information Security	
Is there an ability to audit access to the data?	Yes/No (*Is there a way to monitor who accesses information within your internal systems*)
Will access to data be controlled? By what roles?	*What processes are in place so that information is only accessed by those that need to access it.*
Provide details of the security and audit measures e.g. username& password, smartcard, key locked filing cabinet, secure token, restricted access to shared drives/folders etc.	*Describe what happens to allow staff access to the different systems you have in place wthin your organisation ie smartcard and password access, locked doors to rooms that hold lloyd George notes, do you have protected HR folders on the shared drive etc*
Are there any BCP and emergency recovery protocol proposed/existing for the new process/service?	*What plans do you have in place in the event this new process fails?*

Record of Outcome and Sign Off				
What are the Risks identified for this process/service:				
Describe source of risk and nature of potential impact on individuals including any associated compliance and corporate risk as necessary		Likelihood of occurrence	Severity of harm	Overall risk
Link to related documents		Will data be shared with anyone else?	Yes/No	

THE WESTERHAM PRACTICE

What measures will you put in place to ensure all risks are covered?				
Risk	Options (measures) to reduce or eliminate risk	Effect on Risk	Residual Risk	Measure/Residual Approved By
(List identified risks)		(Reduce or eliminate or accept residual risk)	Low, medium or high	*(Accountable Officer/SIRO)*
Summary actions from this assessment				
DPO Advice provided:				
DPO advice accepted or Overruled (if overruled, state by whom and reasons)				
This DPIA is a one-off/ will kept under review by:	Yes/No (name of who will be reviewing and date of next review)			
Signed off and Dated By Caldicott Guardian:				
Signed off By SIRO and Dated *(if applicable):*				

THE WESTERHAM PRACTICE

APPENDIX C - Short DPIA

Shortened Data Protection Impact Assessment for emergency use, such as pandemics Project use

It is a requirement of the General Data Protection Regulations that all new systems, processes or services have a DPIA conducted prior to go-live to ensure due consideration of data protection by design and default. During the period under which organisations are responding to the COVID-19 pandemic, this short form can be used to capture key elements of the project or system being implemented, **after which a retrospective full DPIA must be completed.**

This questionnaire will still be reviewed by the relevant stakeholders and will be signed off by the **SIRO and Caldicott** and sent to the Data Protection Officer to ensure that the DPIA log is continually updated.

Project/Service Lead contact details	
Senior Responsible Officer for the Project (name, job title, email address, contact details)	

Purpose of the Project/Service
Project/Service Name:

Name of system /application being used:
Details of the system/application in use elsewhere within UK:

Risk assessment and mitigation
Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.*
Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*

Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*
Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?
If the answer is "Yes" to any questions in this section, how are these to be reduced or mitigated?

Once the mitigations are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.

Likelihood *(please tick)*				**Severity** *(please tick)*				
1		Rare	**x**	**1**		Negligible	**=**	
2		Unlikely		**2**		Minor		
3		Possible		**3**		Moderate		
4		Likely		**4**		Major		
5		Almost certain		**5**		Catastrophic		

IG Comments and Recommendations	
Date:	
IG Lead:	

SIGN OFF

THE WESTERHAM PRACTICE

SIRO:	
Date & Signature:	
Caldicott:	
Date & Signature:	

Once completed, and signed off, please send this form to: Practice Manager