DATA PROTECTION IMPACT ASSESSMENT FRAMEWORK

GUIDANCE FOR THE COMPLETION OF A DATA PROTECTION IMPACT ASSESSMENT

For more information on the status of this guidance and template, please contact:	
NHS South, Central and West CSU	Information Governance Team
Approved by	Information Governance Steering Group
Approval Date	25-06-18
Next Review Date	April 2020
Responsibility for Review	Information Governance Team
Contributors	NHS South, Central and West CSU Information Governance Team
Audience	All NHS South, Central and West CSU officers and staff (which includes temporary staff, contractors and seconded staff) and NHS South, Central and West CSU members in their capacity as commissioners. CCG customers are permitted to use both the template and guidance but it is recommended that approval is sought for this from the organisations appropriate committee before adopting. Other customers of NHS South, Central and West CSU are permitted to use both the template and guidance but it is recommended that approval is sought for this from the organisations appropriate committee before adopting

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	05/12/2013	Draft	New document	NHS South CSU Information Governance team
0.2	12/12/2013	Draft	Amendment following Beverly Carter and Jackie Thomas comments	NHS South CSU Information Governance team
0.3	24.02.2014	Draft	Amendment following Beverly Carter comments	NHS South CSU Information Governance team
0.4	30.07.14	Draft	Amendment following IG Team comments	NHS South CSU Information Governance team
0.5	19.02.15	Draft	Amendment following IG Team comments	NHS South CSU Information Governance team
0.6	24.09.15	Draft	Amended to refer to NHS South, Central and West CSU	NHS South, Central and West CSU Information Governance Team
1.0	17.03.2016	Final	Approved by SCWCSU IGSG	NHS South, Central and West CSU Information Governance Team
1.1	03.04.16	Final	Amendment following IG Team comments	NHS South CSU Information Governance team
1.2	11.05.2016	Final	Screening questions added as Appendix 1 and referred to in the document	NHS South, Central and West CSU Information Governance Team
1.3	04.07.2016	Final	Updated PIA template added	NHS South, Central and West CSU Information Governance Team
1.3	29.11.16	Final	CSU generic inbox updated	NHS South, Central and West CSU Information Governance Team
2.0	27.03.17	Final	Complete review of PIA template and guidance	NHS South, Central and West CSU Information Governance Team
3.0	23.05.18	Final	Complete review of DPIA templates and guidance	NHS South, Central and West CSU Information Governance Team

CONTENTS

1. INTRODUCTION 5

2. SCOPE 5

3. ROLES AND RESPONSIBILITIES 5

4. KEY PRINCIPLES 6

5 DATA PROTECTION IMPACT ASSESSMENT REVIEW PROCESS 12

6 COMPLETING THE PRIVACY IMPACT ASSESSMENT TEMPLATE 12

7 REVIEW 12

APPENDIX 1: TEMPLATE 12

APPENDIX 2: HOW TO COMPLETE THE TEMPLATE 12

APPENDIX 3: EQUALITY IMPACT ASSESSMENT 13

1. INTRODUCTION

The GDPR introduces a new obligation to complete a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. This is a key element of the new focus on accountability and data protection by design. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

2. SCOPE

This guidance and associated templates is for use within SCW CSU for its own activities. An adapted format is provided for customers to reflect different roles and responsibilities.

3. ROLES AND RESPONSIBILITIES

3.1 Senior Information Risk Owner (SIRO)

The SIRO has ownership of the organisation's information risks and provides assurances to the Executive Management Team. They are responsible for assessing the risks associated with changes to existing systems or the development of new information systems and for providing a final approval to such activities.

3.2 Caldicott Guardian

The Caldicott Guardian can provide advice and guidance where the proposed activity involves the collecting, processing, storage and sharing of Patient or other Personal confidential Data. They should be consulted as part of the DPIA process where necessary and can also provide final approval to proposed activities.

3.3 Deputy Data Protection Officer (DDPO)

Any information risk found when carrying out a Data Protection Impact Assessment that are an amber/red, red or black risk (using the risk matrix below) that cannot be mitigated against are to be reported directly to the NHS England DPO. The Head of Information Governance is the current DDPO.

Impact						
	Very High -5	A	A/R	R	R	B
	High - 4	A	A	A/R	R	R
	Moderate - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Very Likely
		Likelihood				

3.4 NHS South, Central and West CSU Information Governance Team

SCW CSU IG Team can provide a valuable source of advice and guidance throughout the design phase of any new service, process or information asset. The Senior Management Team for the SCW CSU IG team will review any DPIA's concerning SCW CSU activities.

3.5 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are accountable for the information systems under their control and are responsible for managing any risks associated with data flows into and out of those systems and for the quality, security and confidentiality of any data held in them.

3.6 Data Custodians

Data Custodians will:

- ensure that guidance in this document is followed,
- recognise actual or potential risks when new processes are being introduced in their directorate/department,
- consult with their IAOs and SCW CSU IG team to take steps to mitigate risks,
- encourage project/programme leads complete the DPIA template at the initiation stage of a project/process

Managing information risk effectively requires a structured approach involving work areas where accountability sits with senior managers, rather than specialist staff. All staff need to work together to help identify and mitigate information risk.

4. KEY PRINCIPLES

4.1 What is a DPIA

A DPIA is a way to systematically and comprehensively analyse processing activities and help identify and minimise data protection risks. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into organisational processes and ensure the outcome can influence plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, and regularly review it.

The ICO has published detailed guidance ICO DPIA guidance

4.2 Do we need a DPIA?

A DPIA should be done before any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed, a DPIA screens for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says a DPIA must be done where there are plans 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 a DPIA if there are plans to:

- use new technologies; processing involving the use of new technologies, or the novel application of existing technologies (including AI) such as Credit checks, Mortgage / loan applications, Fraud prevention, Insurance underwriting, **Smart technologies (including wearables)**
- use profiling or special category data to decide on access to services; e.g. decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data such as Political parties membership data, Trade Union membership data, **health records processed by Hospitals/health clinics/gym chains, social care records,** Research (including medical research), fraud prevention, application of AI, dating websites/applications
- profile individuals on a **large scale** including hardware/software offering fitness/lifestyle monitoring;
- process biometric data;
- **process genetic data for medical diagnosis, DNA testing or medical research**
- **match data or combine datasets from different sources including monitoring personal use/uptake of statutory services or benefits**
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') examples include list brokering, direct marketing, online tracking by third parties, online advertising, data aggregation/data aggregation platforms, re-use of publically available data;
- track individuals' location or behaviour using social networks, software applications, hardware/software offering fitness/lifestyle/**health monitoring**, online advertising, web and cross-device tracking, data aggregation/data aggregation platforms, eye tracking, data processing at the workplace, data processing in the context of home and remote working, processing location data of employees, loyalty schemes, tracing services;
- profile children or target marketing or online services at them including connected toys and social networks ; or
- **process data that might endanger the individual's physical health or safety in the event of a security breach such as complaint procedures or social care records**

A DPIA should be considered 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. For example, the NHS considers the following as specific situations worthy of a DPIA:

- the requirement for a change of the legal basis for processing data
- replacement of an existing personal data system by new software
- design and development of a system where the data held is on a consent basis
- changes to an existing system where additional personal data will be collected
- a proposal to collect personal data from a new source
- creation or redesign of web-forms for collecting personal data
- plans to outsource business processes involving storing and processing personal data
- intended reuse of information which was originally collected for a limited purpose in a new and unexpected way
- relocation of staff or equipment
- stakeholder Engagement e.g. surveys

Even if there is no specific indication of likely **high risk**, it is good practice to do a DPIA for any major new project involving the use of personal data. It is important to note that the individuals referred to are patient/service users and staff.

4.3 What does systematic and extensive mean?

'Systematic' means that the processing:

- occurs according to a system;
- is pre-arranged, organised or methodical;
- takes place as part of a general plan for data collection; or
- is carried out as part of a strategy

The term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals.

4.4 What does large scale mean?

The GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data

Individual professionals processing patient or client data are not processing on a large scale.

4.5 What is high risk?

Risk in this context is about the potential for any significant physical, material or non-material harm to individuals. To assess whether something is 'high risk', the GDPR is clear that you need to consider both the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk in that sense is part of the job of a DPIA.

4.6 What does significantly affect mean?

It is something that has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way. A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

4.7 Who should carry out a Data Protection Impact Assessment?

A **Controller** is responsible for the DPIA, it can be outsourced but the Controller remains responsible for it.

In most cases SCW CSU will be acting in a '**Processor**' role and not as a 'Controller'. NHS England will almost always be the Controller for all SCW activities.

The NHS England **Data Protection Officer (DPO)** is not able to provide advice and guidance on all NHSE and CSU DPIA's therefore a **deputy DPO** has been identified within SCW to carry out these functions on their behalf. Their advice on the DPIA is required at all times and this will be facilitated via the Senior IG Management Team DPIA panel chaired by the Head of Information Governance for SCW.

We are able to carry out a DPIA as a Processor if we undertake the relevant processing operation. Any request or decision to do this must be agreed with the Deputy DPO in order to determine our specific role in the project/activity and who the key decision makers/Controllers are.

For example, SCW may be asked to provide an analytics solution for a group of Clinical Commissioning Groups (CCG) that will utilise their commissioning data from NHS Digital and ask for it to be combined with data that only exists in the GP systems across their areas. Whilst the CCGs remain joint Controllers with NHS Digital for commissioning data and the GP's remain Controllers for their data, it may be prudent to ask the CSU as the Processor to undertake the DPIA due to the technical nature of the request and the need to identify potential risks and issues that will be common across the Controllers. The DPIA will however require consultation and sign off from the Controllers as a Processor can only act under their instruction and agreement which should never be assumed.

DPIAs should be completed by key project personnel - this could be the project lead, manager, or any other key project team member. It is likely that multiple staff from the project will need to be involved with carrying out the DPIA.

It is essential that the person(s) undertaking the DPIA has clear knowledge of the project, the systems involved and the level of information required, therefore this document is for use by anyone who proposes or develops new systems/upgrades existing systems within the organisation.

4.8 When Should a DPIA Be Completed?

A DPIA can help evidence that data protection by design has been considered by assessing data protection and privacy issues upfront in every activity. It can help ensure compliance with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

The GDPR states that data protection by design should happen:

- ✓ 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- ✓ 'at the time of the processing itself' – i.e. during the lifecycle of your processing activity

It should begin at the initial phase of any system, service, product, or process. It should start by considering the intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure compliance with the data protection principles and protect individual rights. These considerations must cover:

- ✓ the state of the art and costs of implementation of any measures;
- ✓ the nature, scope, context and purposes of your processing; and
- ✓ the risks that your processing poses to the rights and freedoms of individuals

These considerations lead into the second step, where actual technical and organisational measures are put in place to implement the data protection principles and integrate safeguards into the processing.

It would be good practice to begin a DPIA at the same time as developing a service specification or other scoping document involved in the procurement process that you are employing to identify a service provider. Answering many of the questions in the DPIA will help determine the types of information related responses required from potential bidders and will help you decide which provider is best placed to meet the obligations you set out in any contract with them. As the DPIA is a living document it can then be used once the contract has been awarded and through the contract implementation stage to assist you and your service provider evidence the information requirements under the relevant contract.

4.9 What are the underlying concepts of data protection by design and by default?

- a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact
- privacy as the default setting - design any system, service, product, and/or business practice to protect personal data automatically, with privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything
- privacy embedded into design - embed data protection into the design of any systems, services, products and business practices, ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services
- avoid trade-offs and insist on privacy and security
- put in place strong security measures from the beginning, and extend this security throughout the 'data lifecycle' – process the data securely and then destroy it securely
- ensuring visibility and transparency to individuals, such as making sure they know what data is processed and for what purpose(s)
- Respect for user privacy – by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given

4.10 The objective of the DPIA is to avoid the following risks

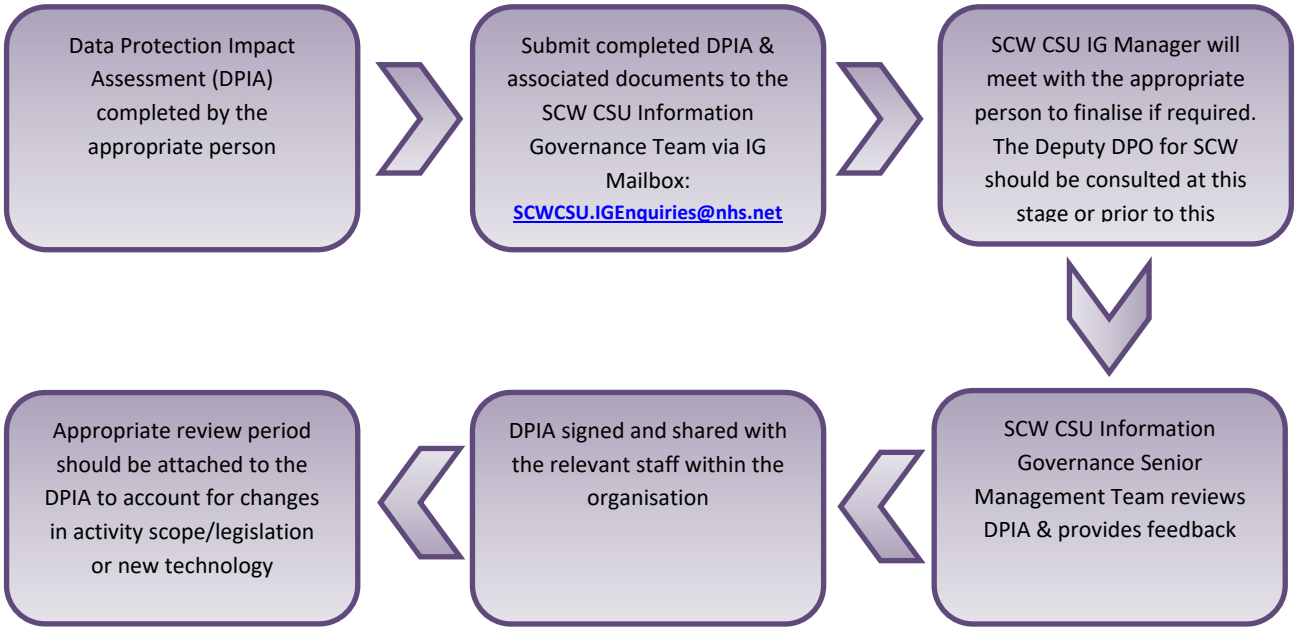
- **Loss of public credibility** as a result of perceived harm to privacy or a failure to meet expectations with regard to the protection of personal information;
- **Imposition of regulatory conditions** as a response to public concerns, with the inevitable cost that entails;
- **The need for system re-design** late in the development stage, and at considerable expense;
- **Collapse of the project, or even of the completed system,** as a result of adverse publicity and/or withdrawal of support by the organisation or one or more key participating organisations;
- **Compliance failure,** under section 157 of the Data Protection Act 2018, the ICO is able to impose a penalty for failing to complete a DPIA when it is mandated to do so under Article 35 of the GDPR. The maximum amount that can be imposed is 10 million Euro's or 2% of total annual worldwide turnover in the case of an undertaking or group of undertakings.

4.11 Outcomes of an Effective DPIA

An effective DPIA will:

- identify the project's privacy impacts
- consider those impacts from the perspectives of all stakeholders
- provide an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it
- identify and assess less privacy-invasive alternatives
- identify ways in which negative impacts on privacy can be avoided
- identify ways to lessen negative impacts on privacy
- clarify the business need that justifies where negative impacts on privacy are unavoidable,
- document the outcome

5 DATA PROTECTION IMPACT ASSESSMENT REVIEW PROCESS



6 COMPLETING THE PRIVACY IMPACT ASSESSMENT TEMPLATE

Once the preparation has been completed and the information collated the DPIA template included as Appendix 1 should be completed. Detailed Guidance is included as Appendix 2.

7 REVIEW

This guidance will be reviewed annually or when changes in legislation or national policy dictate.

8 PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix 3.

Appendix 1: Template

SCW DPIA Template Final version 2.doc

Appendix 2: How to complete the Template

SCW DPIA template guidance v2.0 final dı

Appendix 3: Equality Impact Assessment

EIA form_SCW DPIA Framework and Guida