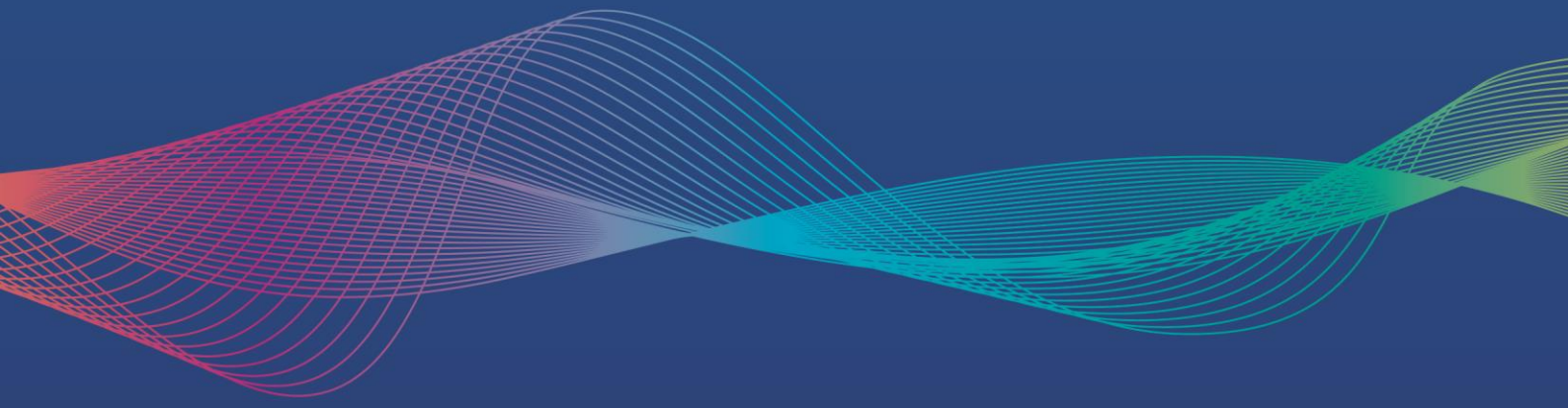
NHS
Midlands and Lancashire
Commissioning Support Unit

Data Protection Impact Assessments – What, When, How?

October 2020



YOUR NHS PARTNER FOR **IMPROVING HEALTH** AND **INTEGRATING CARE**

What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process designed to help an organisation systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of an organisation's accountability obligations under the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679, and when done properly helps you assess and demonstrate how you comply with all of the organisations data protection obligations.

It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

Is a DPIA a Legal Requirement?

Yes, DPIA's are a legal requirement, where the processing of personal (including pseudonymised) data is required and likely to result in a high risk to the rights and freedoms of natural persons. The legal responsibility sits with the Data Controller, a Data Controller is the organisation which determines the purposes and means of the processing of personal data. Failure to carry out a DPIA when required may leave the Data Controller open to enforcement action, including significant fines (10 million euros or 2% global annual turnover if higher).

By considering the risks related to the intended processing before you begin, you also support compliance with another general obligation under Data Protection: Data Protection by Design and Default.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within your organisation. It also ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a 'data protection by design' approach.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations.

However, DPIAs are not just a compliance exercise. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and your organisation.

When is a Full DPIA needed?

A full DPIA must be completed by the data controller for any processing of special-category data on a large scale or when using special category data to help make decisions on someone's access to a service, opportunity, or benefit. Special category data includes any data concerning an individual's health.

However, it is becoming more apparent that as CCGs are commissioning new services and systems there may be occasions which require the DPIA to be completed at commissioner level rather than provider (Data Controller) level.

In some circumstances the CCGs may be directed by NHS England or their respective Integrated Care System (ICS) to undertake a specific programme of work in their area. Therefore the CCG may be best placed to complete the DPIA on behalf of the Data Controllers, i.e., if the same project is being rolled out to each GP practice in their area, it would be more pragmatic to complete once at a CCG level rather than 50+ times by each individual practice/data controller. Due to this fact more than often the responsibility may lie with the commissioners to complete on behalf of the Data Controllers.

To determine whether a full **DPIA** or a **DATA PROTECTION ASSURANCE CHECKLIST** is needed, a **PROJECT OVERVIEW FORM** needs to be completed at the start of the procurement process of any new system, project, or service.

Project Overview

When introducing a new service, process or system, the CCG project lead will need to take the lead on completion of the **Project Overview Form** – It is important that the project lead has a good working knowledge of how data is processed at each stage. The Project Overview form should provide enough detail of the planned service to enable the IG Team to advise on the relevant data protection questions to include in any associated procurement exercise.

In scenarios where data is being processed by an external organisation/provider, if identified at this stage it is important that we have a clear picture of how and why they are processing data. Therefore, a key contact within the external organisation is beneficial. Once the project lead has provided an overview of what they plan to do by completing a Project Overview Form, this should be submitted to the IG Team mlcsu.ig@nhs.net.

Once it has been reviewed, this will determine the next action:

- No DPIA/further documentation needed or
- A Data Protection Assurance Checklist or
- A Full DPIA

Data Protection Assurance Checklist

A Data Protection assurance checklist is required when the CCGs are not processing personal identifiable /pseudonymised data but is the commissioning stakeholder and responsible for completing the due diligence on the project/service/appointed provider. This is a legal requirement under the DPA 2018/ GDPR regulation, determined by the accountability principle.

The Data Protection Assurance Checklist must be reviewed by the CCGs Data Protection Officer and SIRO prior to go live, to ensure the CCG is compliant with the Act and any risks carried by the CCG have been identified. The assurance checklist does not require Caldicott Guardian approval due to the CCG not processing personal identifiable/pseudonymised data.

Full DPIA

A Full DPIA is required when the CCGS are processing personal identifiable/pseudonymised data. The IG Business Partner will support the project lead with the technical, legal and security requirements, and make sure all information is recorded in a plain English and easy to understand form. This may require the project lead to discuss further with customers for more information or even system suppliers to answer some of the more technical questions.

The Full DPIA must be reviewed first by the CCGs Data Protection Officer, then the Caldicott Guardian and Senior Information Risk Owner prior to go live. This is to ensure the CCG is compliant with the Data Protection Act and any risks to the data subjects and those that are carried by the CCG have been identified, mitigated or accepted.

COVID DPIAs

The Civil Contingences Act 2004 (CCA) does not override the Data Protection Act 2018, although it does relax some of the responsibilities that organisations need to have in place when responding to an emergency; in times of emergencies it is important that data protection is not seen as an obstacle and that responders can be supported to manage the incident, taking a pragmatic approach to Data Protection. The Act therefore allows for category 1 & 2 responders to share information formally as part of a culture of co-operation.

For this reason, a shortened DPIA template has been developed by the national Information Governance Network (SIGN Group) to support organisations to very quickly record what they intend to do as a workaround and quickly highlight any glaringly obvious data protection risks.

This enables IG professionals to be in a position to give a speedy response to suggested workarounds whilst being able to assure Senior Information Risk Owners (SIRO) that consideration has been given to the required elements of Data Protection. It also enables IG to have a record of the adhoc data sharing that has taken place and once the emergency has passed, to revisit and complete a full retrospective assessment if the system, service or process will continue post emergency.

COVID-19 Data Sharing Briefing for IC

How Long will it take?

A full DPIA needs to be reviewed by multiple people including the Data Protection Officer, Caldicott Guardian and Senior Information Risk Owner of the Data Controller so it is important that it is in plain English and jargon free. DPIAs are also available to the public under the Freedom of Information Act (It is recommended that a list of completed DPIAs be included on each data controllers website) and so needs to be understandable to a member of the public who has no knowledge of the service or project!

Step by Step Process

Below you will find a step by step visual, easy to follow representation of the process. Feedback loops are shown using the following icon 

Project Lead completes the **Project Outline** and submits to the IG Team for initial review mlcsu.ig@nhs.net

IG Team carry out initial review, identify any missing information/obtain clarification and confirm whether no further documentation is required or if a **Data Protection Assurance Checklist** or **Full DPIA** is needed (KPI: 5 Working Days)

Data Protection Assurance Checklist

IG Business Partner to link in with Project Lead to support with completion

IG Business Partner submits to the CCGs Data Protection Officer for review and sign off

Data Protection Officer undertakes review against legislative requirements and returns to IG Business Partner

IG Business Partner submits to the CCGs SIRO for review and sign off

SIRO undertakes review considering the risks to the organisation in processing or not processing the data for this purpose and returns to IG Business Partner

The IG Business Partner shares with the Data Controller for Assurance

Full DPIA

IG Business Partner to link in with Project Lead to support the legal technical and security questions and fully risk assess the project

IG Business Partner submits to the CCGs Data Protection Officer for review and sign off

Data Protection Officer undertakes review against legislative requirements and returns to IG Business Partner

IG Business Partner submits to the CCGs Caldicott Guardian for review and sign off

Caldicott Guardian undertakes review against impact on data subjects and the risk to their data and returns to IG Business Partner

IG Business Partner submites to the CCGs SIRO for review and sign off

SIRO undertakes review considering the risks to the organisation in processing or not processing the data for this purpose and returns to IG Business Partner

The IG Business Partner transfers the relevant information out of the DPIA to create either a Data Sharing Agreement or Data Processing Agreement

The IG Business Partner to link in with the Data Controller to update the Privacy Notice to reglect any new or change in processing. Informaition Asset register and Data Flows should also be updated.

Once DPIA have been completed the project can 'go live'

An overview of the DPIAs should be avaiable on the CCGs website

Project Lead	MLCSU IG
CCG	Project Lead & MLCSU IG

NHS RightCare

CYBER ESSENTIALS

CIMA
Chartered Institute of Management Accountants
PREMIER PARTNER

disability confident EMPLOYER

FUTURE FOCUSED FINANCE
LEVEL 2 ACCREDITED

CIPFA
CPD ACCREDITED EMPLOYER

CIPS PROCUREMENT EXCELLENCE
Standard Award
Number: 0503 – Valid to: 06/2022

CIPS PROFESSIONAL ETHICS
0604
VALID TO 08/05/2020

aat accredited employer

GCHQ Certified Training

APMG International
Accrediting Professionals

For CyberStrong (our cyber security course)

APPROVED EMPLOYER ACCA
Professional Development

APPROVED EMPLOYER ACCA
Trainee Development - Gold

HSJ VALUE AWARDS 2019
FINALIST
PHARMACY AND MEDICINES OPTIMISATION AWARD

HSJ VALUE AWARDS 2019
FINALIST
CLINICAL SUPPORT SERVICES AWARD

HIGHLY COMMENDED OF THE
30 April 2019
Hilton Metropole, Birmingham
goawards.co.uk
UK PUBLIC PROCUREMENT NATIONAL AWARDS

west midlands ACADEMIC HEALTH SCIENCE NETWORK
Mental Health Innovation Award 2017
Innovative Organisation of the Year 2016

HSJ VALUE AWARDS
Winner: Value and improvement in use of IT to drive value in non-clinical support services 2016 (with Birmingham CrossCity CCG)

PENNA
PEN National Awards 2016
Re:thinking the experience
Winner: Commissioner of the Year 2016

Get to know us or get in touch

mlcsu

Midlands and Lancashire Commissioning Support Unit

midlandsandlancashirecsu.nhs.uk