DATA PROTECTION IMPACT ASSESSMENT POLICY

South Lincolnshire Clinical Commissioning Group
South West Lincolnshire Clinical Commissioning Group

Reference Number:	IG 07
Version:	3.0
Name of Originator/.Author & Organisation	Information Governance, Optum Commissioning Support Services
Name of responsible committee	SLT
Responsible Executive Lead:	Liz Ball - Executive Nurse/ Director of Quality
Date Approved By SLT	21st March 2019
Review date:	March 2021
Target Audience:	All staff
Distributed via:	Intranet & Website

Contents

VERSION RECORD			
Version	**Date**	**Status**	**Comment**
3.0	February 2019	Draft	GDPR complaint policy

1. Introduction

A Data Protection Impact Assessment (PIA) is a mandatory requirement under the Data Protection Act 2018 which helps assess privacy risks in the collection, use and disclosure of personal information. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, a declaration of incompatibility with the Human Rights Act, or prohibitive costs in retro-fitting a system to ensure legal compliance or address community concerns about privacy.

This template is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project, building data protection compliance in from the outset rather than bolting it on as an afterthought. This document details the process for conducting a Data Protection Impact Assessment (DPIA) through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated.

A DPIA must be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset being is introduced.

Completion of a DPIA will be built into the organisational business approval and procurement processes. A DPIA must be completed before any high risk data processing takes place.

Completion of a DPIA must be undertaken in the following circumstances:

- introduction of a new paper or electronic information system to collect and hold personal data;
- update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- changes to an existing system where additional personal data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements

This list is not exhaustive.

Must do's

All unmitigated risks to be notified to the ICO.

DPIAs must be published as part of the CCGs transparency materials

Any systems which do not identify individuals in any way do not require a DPIA to be performed. However, it is important to understand that what may appear to be "anonymised" data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals.

The Information Governance team in Optum Commissioning Support Services will advise any services regarding whether a DPIA needs to be completed and support them with review of the DPIA template.

The template is that agreed for use across public sector organisations across Lincolnshire.

Because organisations vary greatly in size, the extent to which their activities intrude on privacy and their experience in dealing with privacy issues makes it difficult to write a 'one size fits all' guide. It is important to note now that not all of the information provided in this guide will be relevant to every project assessed and further discussion may be required with the Information Governance lead within the CCG or with the Information Governance team in Optum CSS.

2. Who is responsible for completing a DPIA?

Any person who is responsible for introducing a new or revised service or changes to a new system process or information asset (the Information Asset Owner (IAO) is responsible for ensuring the completion of a DPIA. This is usually the project manager.

The Information Governance Lead within the CCG or the Information Governance team in Optum CSS can be consulted at the start of the design phase of any new service, process, purchase of implementation of an information asset[1] etc. so that they can advise on the need and procedures for completing the DPIA.

Data Protection Impact Assessment outcomes should be routinely reported in the organisation and raised through the appropriate project/programme board. Significant issues should be raised with the CG/SIRO in order for a risk assessment to be performed. The CCG IG lead is responsible for ensuring appropriate reporting of DPIAs is undertaken. Final approval of DPIAs is the responsibility of the CCG. It is essential that risks are highlighted, owned and mitigated appropriately by the CCG. The CCG IG Lead is responsible for maintaining a register of DPIA's including their status.

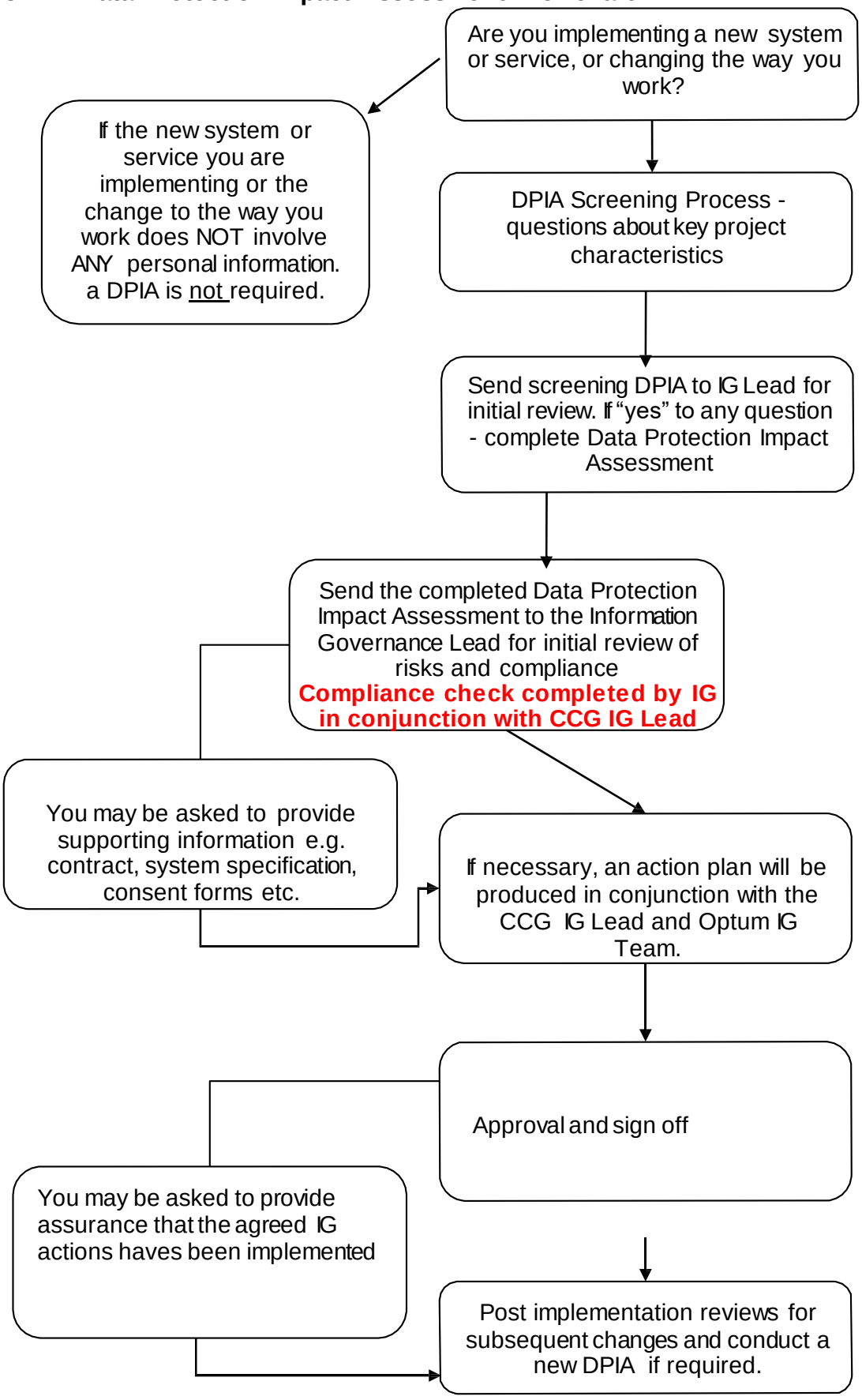
The Role of the Information Asset Owner: a Practical Guide (Extracts)

Information Asset Owner (IAO) is a mandated role and the individual(s) appointed are responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

Information Asset Owners must report to the CCG IG lead so that any concerns arising as a result of DPIAs can be discussed and escalated appropriately.

As well as being a mandatory requirement completing DPIAs brings significant benefits. It provides a common, consistent and unambiguous understanding of what information the CCG holds, how important it is, how sensitive it is, how accurate it is, how reliant the organisation is on it, and who is responsible for it.

3. Data Protection Impact Assessment Flowchart



4. Stages of a PIA

- **The initial screening questions**

This section is to be completed by the service manager or project lead responsible for delivering the proposed change.

The purpose of the screening questions is to ensure that a further DPIA assessment is required and ensure that the investment in the organisation is proportionate to the risks involved**. If response to any of the questions is "yes" then an initial Data Protection Impact Assessment should be considered.**

A meeting with the CCG Information Governance lead should be arranged to review the responses and discuss whether a stage 2 assessment should be completed. The Optum Information Governance Team will support this process as requested by the CCG IG Lead.

- **Data Protection Impact Assessment**

The responses to the screening questions will give an indication as to the appropriate scale of the DPIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

To be completed by the service manager or project lead responsible for delivering the proposed change. The completed form will be assessed by the CCG Information Governance Lead who will advise on the next stage. There are three possible outcomes:

1. The DPIA is incomplete and will have to be repeated or further information obtained.
2. The screening process has not identified any DPIA concerns and the process is complete
3. The screening process has identified a DPIA is required.
   This section includes an explanation of the data flows – the collection use and deletion of personal data should be described.

    - **Compliance Checklist**

The Data Protection Impact Assessment also contains data mapping template and data protection and privacy law compliance checks which need to be considered by the IG lead. The checklist reviews the Data Protection Principles in order for each to be considered and should be completed by the DPIA reviewer.

.

- **Full-Data Protection Impact Assessment**

Where the initial DPIA screening identifies processing of personal data and any associated risks, an action plan should be developed on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities and timescales and will be given to the CCG Information Governance Lead for discussion within relevant Information Governance/other groups who will be responsible for the provision of expert advice and for ensuring that the remedial actions are implemented within agreed timescales. All unmitigated risks to be addressed appropriately and detailed fully and accepted by the CCG.

The organisations Caldicott Guardian and/or Senior Information Risk Owner (SIRO) should be included at an early stage to ensure adequate consultation on the DPIA. In some circumstances the Data Protection Officer for the CCG will be contacted for support and advice.

Appendix 1

DPIA Template
For SL & SWL CCGs to access the template please go to your intranet and select DPIA under D in the staff handbook or contact your CCG Information Governance Lead.
For LE CCG to access the template visit Leon, your intranet site.

Extract from template - Privacy Impact Assessments (PIAs) are required in order to meet national Information Governance requirements and UK data protection legislation including GDPR. Please complete this in accordance with your organisations Information Governance policies.

This tool consists of two parts: Part 1 being a PIA and Part 2 is a full Data Protection Impact Assessment (DPIA)

Part 1 - Purpose of Undertaking a PIA
A PIA is required as a screening tool to establish whether there is a risk to privacy and a full DPIA is required, therefore the PIA must be completed in the first instance.

If the project / processes does not affect personal data in any way then the PIA will be very short - organisations must still demonstrate that they have considered individuals privacy as part of standard business practices i.e. Data Protection by Design and Default.

Part 2 - Purpose of Undertaking a DPIA
A DPIA must be completed once a requirement has been established to assess the risk to privacy of introducing the new system / service and to identify mitigation factors to reduce the risk to an acceptable level.

Once completed, this document should be held as part of the project documentation and a copy held by the organisations IG lead or DPO.