

Document filename:	Data Protection Impact Assessment – Screening Questionnaire
Directorate / Programme	
Document Reference	Status
Information Asset Owner	Version
Author	Version issue date

Data Protection Impact Assessment – Screening Questionnaire

Document management

Revision History

Version	Date	Summary of Changes

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Title	Date	Version

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

About this Document

This document is a 'Screening Questionnaire' to decide if a full data Protection Impact Assessment (DPIA) is necessary. It has been produced by NHS Digital in line with:

- UK Data Protection Bill (14 Sep 17)
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- Working Party 29 guidelines determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, wp248rev.01

Templates will be updated when Information Commissioner’s Office (ICO) guidance reflecting the new legislation is issued (Post May 2018).

Supplementary guidance issued by the ICO can be found here:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

The full DPIA template and accompanying Guidance Notes can be found here;
<http://teams2/sites/IGPG/Useful%20Tools/Forms/AllItems.aspx?RootFolder=%2Fsites%2FIGPG%2FUseful%20Tools%2FTemplates&FolderCTID=0x01200005E2C33E5E36524AAB1D7DA3151E3268&View={E20FDCA0-3451-489E-B0EE-702A7947C9F6}>

How to Use This Document

A DPIA is not required to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. A DPIA is only mandatory where processing is “*likely to result in a high risk to the rights and freedoms of individuals*”.

In cases where it is not clear whether a DPIA is required one is to be carried out regardless. It is a useful tool. To help NHS Digital comply with data protection law.

To understand if you will be processing personal data and special categories of personal data under GDPR, complete the data items table below.

Data Items <i>[Information relating to the individual]</i>	Yes	No
Personal Data		
Name		
Address		
Postcode		
DOB		
Age		
Sex		
Marital Status		
Gender		

Living Habits		
Professional Training / Awards		
Income / Financial / Tax Situation		
Email Address		
Physical Description		
General Identifier e.g. NHS No		
Home Phone Number		
Online Identifier e.g. IP Address / Event Logs		
Website Cookies		
Mobile Phone Number / Device Number		
Device IMEI No		
Location Data (Travel / GPS / GSM Data)		
Device MAC Address (Wireless Network Interface)		
Special categories of Personal Data		
Physical / Mental Health or Condition		
Sexual Life / Orientation		
Family / Lifestyle / Social Circumstance		
Offences Committed / Alleged to have Committed		
Criminal Proceedings / Outcomes / Sentence		
Education / Professional Training		
Employment / Career History		
Financial Affairs		
Religion or Other Beliefs		
Trade Union membership		
Racial / Ethnic Origin		
Biometric Data (Fingerprints / Facial Recognition)		
Genetic Data		

If the answer to any of the data items is “Yes” then personal data is being processed and the following nine questions need to be answered.

If all the answers are “No” then you do not need to answer the nine questions and the DPIA screening questionnaire is complete.

If personal data is being processed, use the questionnaire below to determine whether a full DPIA is necessary.

Should the answer to any screening question be “Yes” but the IAO believes the processing not to be “likely to result in a high risk” NHS Digital must justify and document the reasons for not carrying out a DPIA and include/record views of the Data Protection Officer.

Not Necessary. If “N/A” then a full DPIA may not be necessary but the completed questionnaire itself is evidence that the processing was properly considered.

Serial	Section	Yes	N/A	Unsure (Explain)
1.	Does the proposal involve any evaluation or scoring including profiling & predicting using information about a person?			
2.	Does the proposal involve any automated decision making which has a legal or similar legal effect e.g. whether to employ an individual, grant them a loan or offer medical insurance?			
3.	Does the proposal involve any systematic monitoring: processing used to observe, monitor or control individuals, including data collected through networks e.g. employees’ activities, including the monitoring of the employees’ work station, internet activity; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation; includes internet tracking and profiling for behavioural advertisement?			
4.	Does the proposal involve any sensitive information or information of a highly personal nature e.g. health?			
5.	Does the proposal involve data processed on a large scale? Large scale is not defined but should consider: A) The number of data subjects, either as a specific number or as a proportion of the relevant population. B) The volume of data and/or the range of different data items processed. C) The duration, or performance of the data processing activity. D) The geographical extent of the processing activity. Processing of patient data in the regular course of business by a hospital would be classed as “large scale” while processing of patient data by an individual physician would not.			

6.	Does the proposal involve any matching or combining of datasets? i.e. matching two or more data processing operations performed for different purposes in a way that would exceed the reasonable expectations of an individual.			
7.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where an imbalance in the relationship between the position of the individual and the controller (NHS Digital) can be identified.			
8.	Does the proposal involve any innovative use or applying new technological or organisational solutions e.g. combining use of finger print and face recognition for improved physical access control?			
9.	Does the proposal involve any processing which in itself 'prevents data subjects from exercising a right or using a service or contract' e.g. determining eligibility based on an individual's circumstances?			