

## Data Protection Impact Assessment Procedure

Author	Steve Creighton, Senior IG Officer
Date approved	TBC
Committee	Information Governance Committee
Version	1
Review date	TBC

## Version history

Version	Date	Reviewer	Description	Circulation
1	August 2018	Leeds CCG		

## Contents

1. Introduction .....	4
2. Data Protection Impact Assessments .....	4
3. Purpose of a DPIA .....	5
4. Responsibilities .....	5
5. Is a DPIA required for every project? .....	6
6. When should I start a DPIA? .....	6
7. Publishing DPIAs .....	6
Data Protection Impact Assessment (DPIA) Screening Questions .....	8
Data Protection Impact Assessment (DPIA) .....	9
Appendix A - Example risks.....	24
Appendix B – Supporting Documents.....	<b>Error! Bookmark not defined.</b>
Appendix C - Glossary .....	25
Appendix D - Further information .....	29

## 1. Introduction

Data Protection Impact Assessments (DPIAs)<sup>1</sup> are required under the General Data Protection Regulation (EU) 2016/679, where health data is being used in a manner that it either is identifiable or there is a risk of an individuals' identity being revealed. A DPIA should also be considered where other personal data, for example data about individual staff, is being used in a way that could poses a high level of risk regarding the privacy of those individuals.

DPIAs aid organisations in determining how a particular project, process or system may affect the privacy of the individual. This procedure consists of DPIA Screening Questions and Data Protection Impact Assessment which are designed to enable an assessment *prior to* new services or new data processing/sharing systems being introduced. A DPIA is not effective when key decisions have already been taken. If an assessment is suggested, it should be seen as dynamic and subject to review with any significant change.

DPIAs identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow for the identification and remedy problems at an early stage, reducing potential distress, subsequent complaints and the associated costs and damage to reputation that might otherwise occur.

It is important to consider whether a DPIA is required as soon as the objectives/aims of the project are identified to examine what is required to successfully meet these and how it is envisaged this will happen, whilst ensuring privacy of individuals to which the data relates.

Conducting a DPIA should not be complex or time consuming, if it is given due regard at an early stage.

## 2. Data Protection Impact Assessments

DPIAs identify privacy risks, foresee problems and bring forward solutions. A successful DPIA will:

- identify and manage risks in respect of privacy of personal information(see Appendix A for examples)
- avoid inadequate solutions to privacy risks
- avoid unnecessary costs
- avoid loss of trust and reputation
- inform the organisation's communication strategy
- meet or exceed legal requirements

The Information Commissioners Office (ICO) has produced guidance materials on which this procedure is based (see Appendix D).

DPIAs should demonstrate that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable data.

---

<sup>1</sup> DPIAs were previously known as Privacy Impact Assessments under the Data Protection Act 1998.

### **3. Purpose of a DPIA**

A DPIA should serve to:

- identify privacy risks to individuals
- identify privacy and Data Protection compliance liabilities
- protect the organisations reputation
- instil public trust and confidence in your project/product
- avoid expensive, inadequate “bolt-on” solutions
- inform your communications strategy

### **4. Responsibilities**

Responsibility for ensuring that a Data Protection Impact Assessment is considered and where appropriate, completed, resides with the manager(s) leading the introduction of new systems, data sharing or projects. Completion of the [Screening Questions](#) also serves to evidence that this has been considered.

Line Managers are responsible for ensuring that permanent and temporary staff and contractors are aware of the Data Protection Impact Assessment procedure.

There is an expectation that partner organisations/third parties involved in supplying/providing services contribute the necessary technical information for the Data Protection Impact Assessment.

This guidance therefore applies to all staff and all types of information held by the organisation. This procedure should be read in conjunction with the organisation’s Information Governance (IG) policies.

## 5. Is a DPIA required for every project?

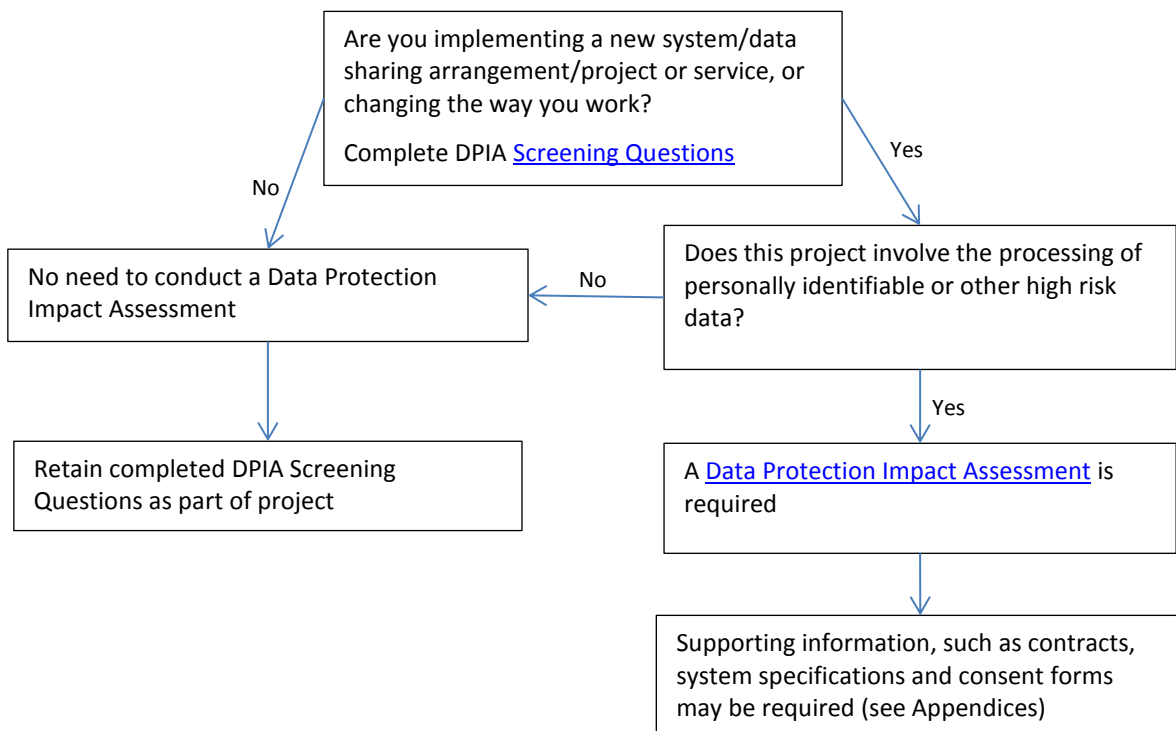


Figure 1

DPIAs should be completed where a system/data sharing/project includes the use of personal data, where there is otherwise a risk to the privacy of the individual, utilisation of new or intrusive technology, or where private or sensitive data which was originally collected for a limited purpose will be reused in a new and 'unexpected' way.

## 6. When should I start a DPIA?

DPIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed
- you know what you want to do
- you know how you want to do it
- you know who else is involved

It **must** be completed before:

- decisions are set in stone
- you have procured systems/services
- you have signed contracts/Memorandum of Understanding/agreements
- while you can still change your mind

## 7. Publishing DPIAs

All DPIA's are to be included within the organisation's Publication Scheme and must therefore be presented to the Governance Lead once they have received approval.

It is acknowledged that DPIA's may contain commercial sensitive information such as security measures or intended product development. It is acceptable for such items to be redacted but as much of the document should be published as possible.

## **Data Protection Impact Assessment (DPIA) Screening Questions**

The below screening questions should be used inform whether a DPIA is necessary. This is not an exhaustive list therefore in the event of uncertainty, completion of a DPIA is recommended.

<b>Title</b>	Click here to enter text.
<b>Brief description</b>	Click here to enter text.

*Screening completed by*

<b>Name</b>	Click here to enter text.
<b>Title</b>	Click here to enter text.
<b>Department</b>	Click here to enter text.
<b>Email</b>	Click here to enter text.
<b>Date</b>	Click here to enter text.

Marking any of these questions is an indication that a DPIA is required:

<b>Screening Questions</b>		<b>Tick</b>
1	Will the project involve the collection of new identifiable or potentially identifiable data about individuals?	<input type="checkbox"/>
2	Will the project compel individuals to provide data about themselves? i.e. where they will have little awareness or choice.	<input type="checkbox"/>
3	Will identifiable data about individuals be shared with other organisations or people who have not previously had routine access to the data?	<input type="checkbox"/>
4	Are you using data about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development.	<input type="checkbox"/>
5	Where data about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress.	<input type="checkbox"/>
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	<input type="checkbox"/>
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	<input type="checkbox"/>
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition or automated decision making.	<input type="checkbox"/>
9.	Is a service being transferred to a new supplier (or recontracted) and the end of an existing contract	<input type="checkbox"/>
10.	Is processing of identifiable/potentially identifiable data being moved to a new organisation (but with same staff and processes)	<input type="checkbox"/>

***Please retain a copy of this questionnaire within your project/system documentation.***

***Please note that once completed the following sections (1 to 4) should be extracted from the rest of this document prior to being included within the Publication Scheme.***



## Data Protection Impact Assessment (DPIA)

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

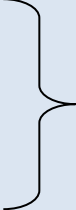
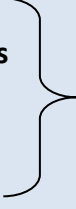
### Section 1

#### System/Project General Details

<b>System/project/process (referred to thereafter as 'project') title:</b>	Click here to enter text.	
<b>Objective:</b>	Click here to enter text.	
<b>Detail:</b> Why is the new system/change in system required? Is there an approved business case?	Click here to enter text.	
<b>Stakeholders/Relationships /Partners:</b> Please outline the nature of such relationships and the corresponding roles of other organisations.	Click here to enter text.	
<b>Other related projects:</b>	Click here to enter text.	
<b>Project lead:</b>	<b>Name:</b>	Click here to enter text.
	<b>Title:</b>	Click here to enter text.
	<b>Department:</b>	Click here to enter text.
	<b>Telephone:</b>	Click here to enter text.
	<b>Email</b>	Click here to enter text.
<b>Information Asset owners/Administrators (if applicable)</b>		
<b>Information Asset Owner:</b> All information systems/assets must have an <a href="#">Information Asset Owner (IAO)</a> . IAO's should normally be a Head of Department/Service.	<b>Name:</b>	Click here to enter text.
	<b>Title:</b>	Click here to enter text.
	<b>Department:</b>	Click here to enter text.
	<b>Telephone:</b>	Click here to enter text.
	<b>Email</b>	Click here to enter text.
<b>Information Asset Administrator:</b> Information systems/assets may have an <a href="#">Information Asset Administrator (IAA)</a> who reports the IAO. IAA's are normally System Managers/Project Leads.	<b>Name:</b>	Click here to enter text.
	<b>Title:</b>	Click here to enter text.
	<b>Department:</b>	Click here to enter text.
	<b>Telephone:</b>	Click here to enter text.
	<b>Email</b>	Click here to enter text.

## Section 2

### Data Protection Impact Assessment Key Questions

	Question	Response
1.	<p><b>Will the project use identifiable or potentially identifiable data in any way?</b> If answered 'No' then a DPIA is not normally suggested.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, who will this data relate to:</p> <p><input type="checkbox"/> Patient <input type="checkbox"/> Staff <input type="checkbox"/> Other: <a href="#">Click here to enter text.</a></p>
2.	<p><b>Please state purpose for the processing of the data:</b> For example, patient care, commissioning, research, audit, evaluation.</p>	<p><a href="#">Click here to enter text.</a></p>
3.	<p><b>Please tick the data items that are held in the system</b></p> <p><b>Personal</b> </p> <p><b>Special categories of personal data (sensitive data)</b> </p>	<p><input type="checkbox"/> Name <input type="checkbox"/> Address  <input type="checkbox"/> Post Code <input type="checkbox"/> Date of Birth  <input type="checkbox"/> GP Practice <input type="checkbox"/> Date of Death  <input type="checkbox"/> NHS Number <input type="checkbox"/> NI Number  <input type="checkbox"/> Passport Number <input type="checkbox"/> Pseudonymised Data  <input type="checkbox"/> Online Identifiers (e.g. IP Number, Mobile Device ID)</p> <p><input type="checkbox"/> Health Data <input type="checkbox"/> Trade Union membership  <input type="checkbox"/> Political opinions <input type="checkbox"/> Religion  <input type="checkbox"/> Racial or Ethnic Origin <input type="checkbox"/> Sex life and sexual orientation  <input type="checkbox"/> Biometric Data <input type="checkbox"/> Genetic Data</p> <p><input type="checkbox"/> Other:</p>
4.	<p><b>The data of approximately how many individuals will be affected?</b></p>	<p><input type="checkbox"/> 1-10  <input type="checkbox"/> 10-100  <input type="checkbox"/> 100-1000  <input type="checkbox"/> 1000-10 000  <input type="checkbox"/> 10 000-100 000  <input type="checkbox"/> 100 000+  <input type="checkbox"/> Unable to ascertain <a href="#">Click here to enter text.</a></p>
5.	<p><b>Have the individuals been informed of this Data Processing activity</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk) If yes, please specify: <a href="#">Click here to enter text.</a></p>

	Question	Response
6.	<p><b>Will this activity create a new Information Asset for the Practice?</b></p>	<p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If yes</p> <p><b>Has an Information Asset Owner been identified and does the Information Asset and Data Flow Register require updating?</b></p> <p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If yes, include the completed Information Asset Register New Entry Form.</p> <p>Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset?</p> <p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review.</p>
7.	<p><b>Who will be the Data Controller for this activity?</b> The data controller is the individual or organisation who is responsible for determining the reason for the data processing activity, who may not be the “holder” of the data</p>	<p>Click here to enter text.</p>
8.	<p><b>Will a third party be processing data as part of this activity</b></p>	<p><input type="checkbox"/> Yes <span style="margin-left: 200px;"><input type="checkbox"/> No</span></p> <p>If “Yes” please ensure that the <b><u>Data Protection Impact Assessment Key Questions for Providers/Processors</u></b> section of this document is filled in by the Provider.</p> <p>Also ensure that either</p> <ul style="list-style-type: none"> <li>a) the third party/supplier contract(s) <b>include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information</b></li> <li>b) Is the contract based on or utilises the NHS standard contract</li> </ul> <p>If neither are done, please records as a risk</p>

	Question	Response
9.	<p><b>What legal basis enables this data processing?</b></p> <p>For more information about conditions for processing, please see the <a href="#">ICO's GDPR website</a>.</p>	<p>Personal data (identifiers and potentially identifiable data):</p> <p><input type="checkbox"/> Consent: Click here to enter text.</p> <p><input type="checkbox"/> Relating to a contract: Click here to enter text.</p> <p><input type="checkbox"/> Legal obligation: Click here to enter text.</p> <p><input type="checkbox"/> Vital interests: Click here to enter text.</p> <p><input type="checkbox"/> Public task: Click here to enter text.</p> <p><input type="checkbox"/> Other: Click here to enter text.</p> <p>Special categories of personal data (sensitive data), <i>if applicable</i>:</p> <p><input type="checkbox"/> Consent: Click here to enter text.</p> <p><input type="checkbox"/> Medical related: Click here to enter text.</p> <p><input type="checkbox"/> Public Health: Click here to enter text.</p> <p><input type="checkbox"/> Employment related: Click here to enter text.</p> <p><input type="checkbox"/> Vital interests: Click here to enter text.</p> <p><input type="checkbox"/> Already public: Click here to enter text.</p> <p><input type="checkbox"/> Legal claim related: Click here to enter text.</p> <p><input type="checkbox"/> Substantial public interest: Click here to enter text.</p> <p><input type="checkbox"/> Other: Click here to enter text.</p>
10.	<p><b>Are you relying on individuals (patients/staff) to explicit consent to the processing of personal identifiable or sensitive data?</b></p> <p>Please provide copies of any consent documentation that will be used, including patient information leaflets</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No (skip next question)</p> <p>How will consent be obtained and by whom? Click here to enter text.</p> <p>Will the consent cover all proposed processing and sharing/disclosures? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If no, please detail: Click here to enter text.</p>
11.	<p><b>If you are relying only on consent, did you consider any other legal basis?</b></p> <p>Please be aware that consent may not be the best legal basis to use under many circumstances due to the strengthened rights it gives individuals over their data.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> N/A</p> <p>If no, please detail why: Click here to enter text.</p>
12.	<p><b>Who will have access to the data within the project?</b></p> <p>Please refer to roles/job titles/organisations.</p>	<p>Click here to enter text.</p>
13.	<p><b>Have consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of the data for this project?</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk)</p> <p>If yes, please specify: Click here to enter text.</p>

	Question	Response
14.	<p><b>Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?</b></p> <p>The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously)</p>	<p><input type="checkbox"/> Yes (please record as a risk)      <input type="checkbox"/> No</p> <p>If yes, please provide a data flow diagram showing how identifiable information would flow and ensure this is added to the practice Information Asset and Data Flow Register (see Information Assets and Data Flows section).</p>
15.	<p><b>Has stakeholder engagement taken place?</b></p>	<p><input type="checkbox"/> Yes      <input type="checkbox"/> No (please record as a risk)</p> <p>If yes, how have any issues identified by stakeholders been considered?  <a href="#">Click here to enter text.</a>  If no, please outline any plans in the near future to seek stakeholder feedback:  <a href="#">Click here to enter text.</a></p>
16.	<p><b>Does the project involve any new data sharing between stakeholder organisations?</b></p>	<p><input type="checkbox"/> Yes (consider if this will be a risk)      <input type="checkbox"/> No</p> <p>If yes, please describe:  <a href="#">Click here to enter text.</a>  Please provide a high level data flow diagram showing how identifiable information would flow.</p>
17.	<p><b>Does the project involve the collection of data that may be unclear or intrusive?</b></p> <p>Are all data items clearly defined? Is the data collected limited to a specific set of predefined categories?</p>	<p><input type="checkbox"/> Yes (please record as a risk)      <input type="checkbox"/> No</p> <p>If yes, please explain:  <a href="#">Click here to enter text.</a></p>
18.	<p><b>What are the specific retention periods for this data?</b></p> <p>Please refer to the <a href="#">Records Management Code of Practice for Health and Social Care 2016</a> and list the retention period for identifiable project datasets.</p>	<p><a href="#">Click here to enter text.</a></p> <p>If no retention period is specified, please record as a risk</p>
19.	<p><b>Will the data be securely destroyed when it is no longer required?</b></p>	<p><input type="checkbox"/> Yes      <input type="checkbox"/> No (please record as a risk)</p> <p>If no, please detail: <a href="#">Click here to enter text.</a></p>

	Question	Response
20.	Will identifiable/potentially identifiable from the project be released as Open Data (placed in to the public domain)?	<input type="checkbox"/> Yes (please record as a risk) <input type="checkbox"/> No If yes, please describe: <a href="#">Click here to enter text.</a>
21.	Will any personal and/or sensitive data be transferred to a country outside the UK?	<input type="checkbox"/> Yes (please record as a risk) <input type="checkbox"/> No If yes, which data and to which country? <a href="#">Click here to enter text.</a>
22.	Will identifiable data only be handled within the patients' direct care team (in accordance with the <a href="#">Common Law Duty of Confidentiality</a> )?	<input type="checkbox"/> Yes <input type="checkbox"/> No (please consider if this will be a risk) If no, please detail: <a href="#">Click here to enter text.</a>
23.	Will an evaluation of the activity be required?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, has a suitable data set been decided, that specifies what data will be used, where it will be extracted from and what measures are in place (anonymization, pseudonymisation etc) to protect personal data  <input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk)

## Section 2

### Data Protection Impact Assessment Key Questions for Providers/Processors

	Question	Response
1.	<b>Is the Provider/Data Processor registered with the Information Commissioner?</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk) Organisation: <a href="#">Click here to enter text.</a> Data Protection Registration Number: <a href="#">Click here to enter text.</a>
2.	<b>Has the Provider/Data Processor completed and published a satisfactory <a href="#">Data Security and Protection Toolkit submission</a>?</b> Please note that the Data Security and Protection Toolkit replaced the IG Toolkit from 1 April 2018.	<input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk) If yes, please give organisation code and percentage score: <a href="#">Click here to enter text.</a>  <i>DSP/IG Toolkit Score:</i> <input type="checkbox"/> Satisfactory <input type="checkbox"/> Not satisfactory (please record as a risk) <input type="checkbox"/> Satisfactory with Improvement Plan If satisfactory with an improvement plan, please request a copy of the plan and enclose it with this assessment. If not satisfactory, please explain how the service has been procured: <a href="#">Click here to enter text.</a>
3.	<b>Will other third parties (not already identified) have access to the data, or act as Provider/Data Processors?</b> Include any external organisations. <b><u>Please ensure any third party organisation that will have access to this data also complete a DPIA.</u></b>	<input type="checkbox"/> Yes (please consider as a risk) <input type="checkbox"/> No If so, for what purpose? <a href="#">Click here to enter text.</a>  Please list organisations and by what means of transfer: <a href="#">Click here to enter text.</a>
4.	<b>Where will the data be kept/stored/accessed?</b> Where applicable, please refer to data flow diagram.	<a href="#">Click here to enter text.</a>
5.	<b>Please indicate all methods in which data will be transferred</b>	<input type="checkbox"/> Fax <input type="checkbox"/> Email (Unsecure/Personal) <input type="checkbox"/> Email (Secure/nhs.net) <input type="checkbox"/> Internet (unsecure – e.g. http) <input type="checkbox"/> Telephone <input type="checkbox"/> Internet (secure – e.g. https) <input type="checkbox"/> By hand <input type="checkbox"/> Courier <input type="checkbox"/> Post – track/traceable <input type="checkbox"/> Post – normal <input type="checkbox"/> Software <input type="checkbox"/> Mobile app <input type="checkbox"/> Other: <a href="#">Click here to enter text.</a>
6.	<b>How will the data be kept up to date and checked for accuracy and completeness?</b>	<a href="#">Click here to enter text.</a>

7.	<p><b>Please outline how individuals will be informed and kept informed about how their data will be processed.</b></p> <p>A copy of the <a href="#">privacy notice and/or leaflets</a> must be provided.</p>	<p>Click here to enter text.</p>
8.	<p><b>How will consent/non-consent (if applicable), objections or opt-outs be recorded and respected?</b></p>	<p>Click here to enter text.</p> <p>If no provision is in place, please record as a risk.</p>
9.	<p><b>What arrangements are in place to process Subject Access Requests?</b></p> <p>Please include a copy of the SAR procedure if one exists</p>	<p>Click here to enter text.</p> <p>If no provision is in place, please record as a risk.</p>
10.	<p><b>What process is in place for rectifying/blocking data?</b></p> <p>What would happen if such a request were made?</p>	<p>Click here to enter text.</p> <p>If no provision is in place, please record as a risk.</p>
11.	<p><b>Will the processing of data be automated?</b></p> <p>Will the proposed processing of data involved automated means of processing to determine an outcome for the individual?</p>	<p><input type="checkbox"/> Yes (please record as a risk) <input type="checkbox"/> No  <input type="checkbox"/> Not applicable</p> <p>If yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format). Please also detail any profiling that may take place as part through automated processing:  Click here to enter text.</p>
12.	<p><b>Is there a useable audit trail in place for the project?</b></p> <p>For example, to identify who has accessed a record?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk)  <input type="checkbox"/> Not applicable</p> <p>If yes, please outline the audit plan: Click here to enter text.</p>
13.	<p><b>Is there an Access Control Policy in place for the Data/the systems the data is held within?</b></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No (please record as a risk)  <input type="checkbox"/> Not applicable</p> <p>If yes, please outline the policy and how it is implemented:  Click here to enter text.</p>
14.	<p><b>Does the project involve privacy enhancing technologies?</b></p> <p><i>New forms</i> of encryption, two factor authentication and/or pseudonymisation.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If yes, please give details: Click here to enter text.</p>



<p><b>15.</b></p>	<p><b>Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?</b></p> <p>Please note that seeking to influence an individual is considered to be marketing.</p>	<p><input type="checkbox"/> Yes (please record as a risk)      <input type="checkbox"/> No</p> <p>If yes, what communications will be sent?  <a href="#">Click here to enter text.</a></p> <p>Will consent be sought prior to this?  <input type="checkbox"/> Yes      <input type="checkbox"/> No (please record as a risk)</p> <p>If no, please explain why consent is not being sought first:  <a href="#">Click here to enter text.</a></p>
<p><b>16.</b></p>	<p><b>Have the business continuity requirements been considered?</b></p>	<p><input type="checkbox"/> Yes      <input type="checkbox"/> No (please record as a risk)</p> <p><input type="checkbox"/> Business Continuity is not applicable</p> <p>Please explain and either reference how such plans link with the organisational plan or why there are no business continuity considerations that are applicable for this project:  <a href="#">Click here to enter text.</a></p>

**Section 3 – to be completed if a third party has been contracted as a provider or processor**

**Provider IG assurances and caveats checklist (question 1 to be completed by the practice, the remainder to be completed by the Provider/Data Processor)**

	Question	Response
<b>Contract</b>		
1.	<p><b>Has the contract been adapted from the NHS Standard Contract Conditions (or produced through eContract)?</b></p> <p>If this is the case the contract should cover the questions raised in this section.</p> <p>Please ensure that the provider can confirm that the following assurances are in place. If the answer to any of the following is “No” then consider recording this as a risk.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Data Protection Act</b>		
1.	<b>The Provider/Data Processor is registered with the Information Commissioner’s Office?</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
2.	<b>It is clear who are the data controller and Provider/Data Processor and the relationship between the parties.</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.	<b>the legal basis for processing each type of data has been clearly defined</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
4.	<b>the data processor will act only on instruction from the data controller(s) and that no further processing or changed processing will take place without the permission of the data controller</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
5.	<b>The Provider/Data Processor has a publicly available Privacy Notice covering all the data processing relevant to the service</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
6.	<b>The Provider/Data Processor can clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes in accordance with NHS regulations, policies and procedures</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
7.	<b>The Provider/Data Processor can reference measures/controls to prevent unlawful processing</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
8.	<b>The Provider/Data Processor has implemented data protection, confidentiality and information security controls which will be reviewed (at least annually), monitored and assurance of this is provided</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.	<b>All staff contracts for the Provider/Data Processor include relevant data protection and confidentiality clauses (including reference to disciplinary procedures)</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
10.	<b>The Provider/Data Processor confirms that regular IG (at east yearly) training is required of their staff</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
11.	<b>The Provider/Data Processor has implemented a staff Confidentiality Code of Practice</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No

	Question	Response
12.	The Provider/Data Processor is clear regarding responsibilities for: <ul style="list-style-type: none"> <li>• Business continuity</li> <li>• Disaster recovery</li> <li>• Monitoring and audit of access to systems</li> <li>• Records management lifecycle</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No
13.	The Provider/Data Processor is aware of all charges, liability and indemnity, remedies and penalties for breach, failure to keep data securely, in the case of there being an ICO fine for which the Provider/Data Processor is negligent.	<input type="checkbox"/> Yes <input type="checkbox"/> No
14.	The Provider/Data Processor is clear regarding: <ul style="list-style-type: none"> <li>• What happens to records, and in what timeframe</li> <li>• What happens on premature exit for data breach, when it is appropriate to stop processing and under what/who's instruction</li> <li>• Who has responsibility for secure destruction (and under whose instruction)</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>DSP/IG Toolkit</b>		
15.	The Provider/Data Processor has completed the DSP Toolkit	<input type="checkbox"/> Yes <input type="checkbox"/> No
16.	the latest version and correct type of the Toolkit been completed by the Provider/Data Processor	<input type="checkbox"/> Yes <input type="checkbox"/> No
17.	The Provider/Data Processor has published the Toolkit self-assessment at the mandatory satisfactory/compliant level	<input type="checkbox"/> Yes <input type="checkbox"/> No
18.	The Provider/Data Processor's Toolkit submission been independently audited/verified (within the past 12 months) and the audit report shared with the Practice	<input type="checkbox"/> Yes <input type="checkbox"/> No
19.	If the Provider/Data Processor's Toolkit submission is not independently audited, the Provider/Data Processor can confirm they have submitted all the documented evidence as part of its toolkit submission	<input type="checkbox"/> Yes <input type="checkbox"/> No
20.	The Provider/Data Processor conforms with specific information and data standards such as ISO 27001 or a requirement to keep to Toolkit security assertions	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Data Management</b>		
21.	There is a requirement for the Provider/Data Processor to maintain information asset registers, data flow mapping and data sets for extraction and reporting and to share them with the data controller	<input type="checkbox"/> Yes <input type="checkbox"/> No
22.	a data flow map been presented by the Provider/Data Processor i.e. where information will travel from and to, and what the information might contain	<input type="checkbox"/> Yes <input type="checkbox"/> No
23.	The Provider/Data Processor will use minimum data necessary in regards to: The use of NHS Number in line with National Patient Safety Agency requirements. Any Minimum Data Sets required	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Data Sharing Agreement</b>		

	Question	Response
24.	The Provider/Data Processor can specify how data will be shared and what the security requirements around any transfers.	<input type="checkbox"/> Yes <input type="checkbox"/> No
25.	An information sharing agreement is in place	<input type="checkbox"/> Yes <input type="checkbox"/> No A copy of the Information Sharing Agreement to be provided (including a list of organisations).
26.	The Provider/Data Processor has implemented information sharing policies and procedures to make it easier to share information with other partners	<input type="checkbox"/> Yes <input type="checkbox"/> No
27.	The Provider/Data Processor has implemented measures to ensure that relevant personal confidential data is only shared among registered and regulated health and social care professionals who have a legitimate relationship with patient	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Subcontracting (where applicable)</b>		
28.	The Provider/Data Processor is aware that subcontracting is prohibited unless the data controller(s) issue a letter of authorisation specifying as such	<input type="checkbox"/> Yes <input type="checkbox"/> No
29.	The Provider/Data Processor is sub contracting part(s) of this service	<input type="checkbox"/> Yes <input type="checkbox"/> No If the provider is not subcontracting then please move to the next section.
30.	an appropriate data processing contract in place between the Provider/Data Processor and the sub-contractor	<input type="checkbox"/> Yes <input type="checkbox"/> No
31.	The Provider/Data Processor has ensured compliance at all times with obligations equivalent to those imposed on the provider are applied to any subcontractor	<input type="checkbox"/> Yes <input type="checkbox"/> No
32.	The Provider/Data Processor has imposed on its own Sub-Contractors (in the event the Sub-Contractor further subcontracts any of its obligations under the Sub-Contract) obligations that are substantially equivalent to the obligations imposed on the Sub-Contractor	<input type="checkbox"/> Yes <input type="checkbox"/> No
33.	The Provider/Data Processor has ensured rights of audit and inspection in respect of relevant data handling systems to the provider or to the Commissioner or to any person authorised by the provider or by the Commissioner to act on its behalf	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Incidents and breach monitoring</b>		
34.	The Provider/Data Processor has confirmed that it has Information Governance incident reporting policies and procedures in place	<input type="checkbox"/> Yes <input type="checkbox"/> No

	Question	Response
35.	<b>The Provider/Data Processor is aware of the requirement to immediately report serious incidents and to work with the data controller on reporting, monitoring and assistance with the closing of incidents (The Provider/Data Processor may be to subject to a penalty of up to 5% of the contract value where an information breach has occurred, in addition to any fines levied by external organisations)</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
36.	<b>The Provider/Data Processor has implemented measures to ensure all IG incidents are reported in accordance with the HSCIC's Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>FOI</b>		
37.	<b>There is clear responsibility for the sharing of requests for information which may fall under the Freedom of Information Act 2000, Environment Information Regulations 2004 and General Data Protection Regulation/Data Protection Act which clearly states who might take responsibility for clinical audit or audit of the above where required</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Information Governance Structure</b>		
38.	<b>The Provider/Data Processor has nominated an Information Governance Lead and Data Protection Officer</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
39.	<b>The Provider/Data Processor has appointed an Informatics Lead</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
40.	<b>The Provider/Data Processor has appointed or nominated a Senior Information Risk Owner</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No
41.	<b>The Provider/Data Processor has a Caldicott Guardian in accordance with the NHS guidelines and recommendations of the Caldicott Review</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No



**Section 3: Data Protection Impact Assessment Information Governance Review**

Information Governance Review			Response (for completion by project lead)	
Issue	Potential Risk	Recommendation	Agreed Action	Completion (Date and Initials)
1				
2				
3				
4				
5				

*For completion by IG:*

Residual Risk	Main Risk Sources	Main Threats	Main Potential Impacts	Main Controls Reducing the Severity and Likelihood	Severity	Likelihood
1						
2						
3						

**IG review completed by:**  
**Date complete and risk assessed:**

Click here to enter text.  
 Click here to enter text.

**Review date:**

Click here to enter text.

## **Appendix A - Example risks**

### **Risks to individuals**

- i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- ii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- iii. New surveillance methods may be an unjustified intrusion on their privacy.
- iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- vi. Identifiers might be collected and linked which prevent people from using a service anonymously.
- vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- viii. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- x. If a retention period is not established information might be used for longer than necessary.

### **Corporate risks**

- i. Non-compliance with the data protection legislation can lead to sanctions, fines and reputational damage.
- ii. Problems which are only identified after the project has launched are more likely to require expensive fixes.
- iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- iv. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- vi. Data losses which damage individuals could lead to claims for compensation.

### **Compliance risks**

- i. Non-compliance with the Data Protection Act/General Data Protection Regulation (EU) 2016/679.
- ii. Non-compliance with the Common Law Duty of Confidentiality.
- iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- iv. Non-compliance with sector specific legislation or standards.
- v. Non-compliance with Human Rights Act 1998 and Equality Act 2010.



## Appendix C - Glossary

<b>Item</b>	<b>Definition</b>
<b>Anonymised Data</b>	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
<b>Authentication Requirements</b>	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
<b>Caldicott</b>	Seven Caldicott Principles were established following the original reviewed in 1997 and further development in 2013. The principles include: <ol style="list-style-type: none"><li>1. justify the purpose(s)</li><li>2. don't use patient identifiable information unless it is necessary</li><li>3. use the minimum necessary patient-identifiable information</li><li>4. access to patient identifiable information should be on a strict need-to-know basis</li><li>5. everyone with access to patient identifiable information should be aware of their responsibilities</li><li>6. understand and comply with the law</li><li>7. the duty to share information can be as important as the duty to protect patient confidentiality</li></ol>
<b>Common Law Duty of Confidentiality</b>	This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances: <ul style="list-style-type: none"><li>• Where the individual to whom the information relates has consented</li><li>• Where disclosure is in the overriding public interest; and</li><li>• Where there is a legal duty to do so, for example a court order</li><li>• The common law applies to information of both living and deceased patients.</li></ul> The Common Law Duty of Confidentiality persists through the changes to data protection legislation in 2018.
<b>Data Protection Act 1998</b> (due to be repealed in May 2018)	The 1998 Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. It consists of eight principles for data processing.

<b>Data Protection Act 2018</b>	<p>During May 2018, the Act is due to be replaced. The new Act is secondary to the requirements of the GDPR, which means the Act covers national derogations and otherwise supplements the Regulations.</p> <p>The Act specifies the age of 13 years as sufficient to seek consent for the processing of personal data and also identified the Information Commissioner's Office as the national supervisory authority.</p>
<b>Explicit consent</b>	<p>Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.</p> <p>GDPR only recognises explicit consent.</p>
<b>General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information</b>	<p>The GDPR requires that data controllers ensure personal data shall be:</p> <ol style="list-style-type: none"> <li>a) processed lawfully, fairly and in a transparent manner in relation to individuals</li> <li>b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes</li> <li>c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</li> <li>d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay</li> <li>e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals</li> <li>f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures</li> </ol> <p>The implementation of the Regulation completed by 25 May 2018.</p>
<b>Information Asset Administrator (IAA)</b>	<p>There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers</p>
<b>Information Asset Owner (IAO)</b>	<p>These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the</p>

security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.

<b>Implied Consent</b>	<b>Implied consent is unique to the health sector and <i>is no longer recognised under the GDPR (from 25 May 2018)</i>.</b> Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
<b>Information Assets</b>	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
<b>Information Risk</b>	An identified risk to any information asset that the organisation holds. Please see the Risk Policy for further information.
<b>Personal Data</b>	This means data which relates to a living individual which can be identified: <ol style="list-style-type: none"><li>1. from those data, or</li><li>2. from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.</li></ol> It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
<b>Privacy and Electronic Communications Regulations 2003</b>	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
<b>Privacy Invasive Technologies</b>	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
<b>Pseudonymisation</b>	Where patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. GDPR recognises pseudonymised data as personal data with mitigation in

place, if implemented correctly, to protect individuals' privacy and confidentiality.

<b>Records Management: NHS Code of Practice</b>	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
<b>Retention Periods</b>	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
<b>Special categories of personal data (sensitive data)</b>	<p>This means personal data consisting of information as to the:</p> <ul style="list-style-type: none"><li>A. Concerning health, sex life or sexual orientation</li><li>B. Racial or ethnic origins</li><li>C. Trade union membership</li><li>D. Political opinions</li><li>E. Religious or philosophical beliefs</li><li>F. Genetic data</li><li>G. Biometric data</li></ul> <p>Most of these categories were previously referred to as "sensitive data" under the Data Protection Act 1998.</p>
<b>SIRO (Senior Information Risk Owner)</b>	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board.

## **Appendix D - Further information**

*Relevant statutory legislation and law:*

[Common Law Duty of Confidentiality](#)  
[Data Protection Act 2018](#)  
[Freedom of Information Act 2000](#)  
[General Data Protection Regulation \(EU\) 2016/679](#)  
[Human Rights Act 1998](#)  
[Privacy and Electronic Communications Regulations 2003](#)

*Further reading and guidance:*

[Caldicott 2 Review Report and Recommendations](#)  
[Confidentiality Code of Practice](#)  
HSCIC [Code of practice on confidential information](#)  
[Information Security Code of Practice](#)  
[Records Management Code of Practice](#)  
ICO [Anonymisation: managing data protection risk code of practice](#) may help identify privacy risks associated with the use of anonymised personal data  
ICO [Data sharing: code of practice](#) may help to identify privacy risks associated with sharing personal data with other organisations