Data Protection Impact Assessment for

Perioperative Quality Improvement Programme (PQIP)

Document control:

	Name and role	Contact details
Document Completed by	**Jose Lourtie RCoA Clinical Audit Manager**	**jlourtie@rcoa.ac.uk**
Data Protection Officer name	**Sharon Drake**	**sdrake@rcoa.ac.uk**
Document approved by (this should not be the same person that completes the form).	**Sharon Drake**	**sdrake@rcoa.ac.uk**
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z7495398**	

Date Completed	Version	Summary of changes

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	NO		
2	Does your project involve any sensitive information or information of a highly personal nature?	YES		Personal details needed by PQIP are: Name, Date of birth, Postcode, NHS number
3.	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 there is an imbalance in the relationship between the position of the individual and the controller.	NO		
4.	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	NO		
5.	Does your project match data or combine datasets from different sources?	YES		To help PQIP provide an in-depth picture of care, we send personal details (NHS number, date of birth, postcode) to NHS Digital (England), NHS Wales Informatic Service (Patient Episode Database for Wales, Wales) or NHS National Services Scotland (Scotland).
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	YES		The project will link information to individual participants in the study which will tell us if (for example) a patient has been readmitted to hospital after going home. In

				addition NHS Digital, NHS Wales Informatic Service, and National Services Scotland are able to provide us with information about people who may have passed away in order that we do not make contact and cause any distress to relatives. This information includes date and cause of death which is sourced from civil registration data on behalf of the Office for National Statistics. The linked information is returned to the PQIP study team in a digital file. The only identifiable details included in this file are study ID and any information provided on the date and cause of death.
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	NO		
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	NO NO NO NO		

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

Ongoing / Retrospective

Describe the overall aim of the project and the data processing you carry out

The aim is to improve the care and treatment of patients undergoing major surgery in the United Kingdom. We do this by collecting and studying information about the surgery, and then the recovery afterwards. The information collected by PQIP is used by doctors, nurses and medical researchers to: • Produce information on the quality of care received by patients undergoing major surgery in NHS hospitals. • Ensure that any changes or improvements to our services benefit patients • Learn about the best ways in which doctors and nurses can use patient information to improve quality of care • Understand better what happens to patients after they leave hospital after having a major operation, and whether the surgery has had a beneficial effect on their longer-term health.

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians and senior management.

Your must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have.

If you decide against seeking the views of data subjects or their representatives e.g. this would be disproportionate or impracticable, then the justification must be made clear in the box below.

In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

https://pqip.org.uk/content/home

Data Information Flows

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential 'function creep', unforeseen or unintended uses of the data for example data sharing.

Please see attached Dataflow Diagram v.0.2

To help PQIP provide an in-depth picture of care, we send personal details (NHS number, date of birth, postcode) to NHS Digital (England), NHS Wales Informatic Service (Patient Episode Database for Wales, Wales) or NHS National Services Scotland (Scotland). These organisations will link information to individual participants in the study which will tell us if (for example) a patient has been readmitted to hospital after they went home. In addition NHS Digital, NHS Wales Informatic Service, and National Services Scotland are able to provide us with information about people who may have passed away in order that we do not make contact and cause any distress to relatives. This information includes date and cause of death which is sourced from civil registration data on behalf of the Office for National Statistics. The linked information is returned to the PQIP study team in a digital file. The only identifiable details included in this file are the study ID and any information provided on the date and cause of death.

The personal details (listed below) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else outside the NHS or research team.

Personal details needed by PQIP are: Name, Date of birth, Postcode, NHS number

The information collected by PQIP is only used for research after it has been made anonymous.

Details on how we will obtain some of the data collected

We would like to clarify how we will obtain some of the information mentioned in the patient information sheet and consent form for PQIP.

For us to be able to able to access information held by NHS Digital we will send your identifiable data (NHS number, Date of Birth, Postcode and gender) to NHS Digital via a secure trusted data linkage service who will link record level hospital admissions information (Hospital Episode Statistics - HES) to individual participants within the study.

NHS Digital will also link your identifiable data to civil registration data from the Office for National Statistics (ONS) which provides information regarding any deaths of participants occurring over the time of this research.

NHS Digital will then return to us an extract of anonymised HES and ONS data which will only contain your unique PQIP study number. This file will not include any other identifiable data. We will then link the data received from NHS Digital to the information held by PQIP using your PQIP study number. This data linkage enables us to undertake long term follow-up of patients who take part in PQIP, and we will request information from NHS Digital over the next 30 years.

Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

N/A

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether or not you should be collecting the information, examine each data field and decide if you need it.

There are two sections in the table below, one for personal data and one for personal sensitive data items.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
NHS number	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Address	NO		
Postcode	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Date of birth	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
			patients recover for surgery
Date of death	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Age	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Sex	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Marital Status	NO		
Gender	YES		Collecting this data us to match our information with other national sources of information and this will give us a fuller picture of how well patients recover for surgery
Living Habits	NO		
Professional Training / Awards	NO		
Income / Financial / Tax Situation	NO		
Email Address	NO		
Physical Description	NO		
General Identifier e.g. Hospital No	NO		
Home Phone Number	NO		
Online Identifier e.g. IP Address/Event Logs	NO		
Website Cookies	NO		
Mobile Phone / Device No	NO		
Device Mobile Phone / Device IMEI No	NO		
Location Data (Travel / GPS / GSM Data)	NO		
Device MAC Address (Wireless Network Interface)	NO		
Sensitive Personal Data			
Physical / Mental Health or Condition	NO		
Sexual Life / Orientation	NO		

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Family / Lifestyle / Social Circumstance	NO		
Offences Committed / Alleged to have Committed	NO		
Criminal Proceedings / Outcomes / Sentence	NO		
Education / Professional Training	NO		
Employment / Career History	NO		
Financial Affairs	NO		
Religion or Other Beliefs	NO		
Trade Union membership	NO		
Racial / Ethnic Origin	NO		
Biometric Data (Fingerprints / Facial Recognition)	NO		
Genetic Data	NO		
Spare			
Spare			
Spare			

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

We will be collecting this information through a very secure website. Only the hospitals participating, the doctors and nurses working on the NELA in the hospital and the NELA project team will have access to the website. Various validation points are included in the IT system to ensure that the data being entered is accurate, including checking against duplicate NHS Numbers.

Before locking and submitting their data, the local user needs to confirm that all data is correct and that they are aware this indicates they are submitting the data to be used in the project.

Individual's rights

If your project uses personal data you must complete this section.

If your project uses personal data you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Individuals rights (where relevant)	**Describe how you ensure individuals are aware of these rights**	**Describe how you would do this**	**Please copy and paste section of document that states the individuals rights**
Individuals are clear about how their personal data is being used.	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Why does PQIP need my personal details? To help PQIP provide an in-depth picture of your care, we send your personal details (NHS number, date of birth, postcode) to NHS Digital (England), NHS Wales Informatic Service (Patient Episode Database for Wales, Wales) or NHS National Services Scotland (Scotland). These organisations will link information to individual participants in the study which will tell us if you have (for example) been readmitted to hospital after you went home. In addition NHS

			Digital, NHS Wales Informatic Service, and National Services Scotland are able to provide us with information about people who may have passed away in order that we do not make contact and cause any distress to relatives. This information includes date and cause of death which is sourced from civil registration data on behalf of the Office for National Statistics. The linked information is returned to the PQIP study team in a digital file. The only identifiable details included in this file are your study ID and any information provided on the date and cause of death. The personal details (listed below) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else

			outside the NHS or research team. Personal details needed by PQIP are: ✓ Name ✓ Date of birth ✓ Postcode ✓ NHS number The information collected by PQIP is only used for research after it has been made anonymous.
Individuals can access information held about them			
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Can I stop being in the study? You can decide to stop participating at any time – please contact a member of the research team at your local hospital or at the central office listed below.
Rectification of inaccurate information			
Restriction of some processing			
Object to processing undertaken on some legal bases	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Can I stop being in the study? You can decide to stop participating at any time – please contact a member of the research team at your local hospital or at the central office listed below.
Complain to the Information Commissioner's Office;			
Withdraw consent at any time (if processing is based on consent)			
Data portability (if relevant)			

Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	NEED TO ADD THIS
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	NEED TO ADD THIS
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	What would taking part involve? We collect information about you, your surgery, and then your recovery afterwards, both in hospital and at home. This information does not affect the care you receive. Some of this information is provided directly by you, about how you feel about your general health. Other information will be completed by your doctors and nurses, and includes information about the type of surgery, anaesthesia and care you receive before, during and after surgery. If you consent, we would like you to complete three short questionnaires now, before your

			surgery. These will take about 20 minutes to complete. We will then contact you the day after your operation, and again on day 3 after surgery to answer some of these questions again (we will either visit you on the ward, or phone you at home if you have been discharged) – these questions should only take 10 minutes to complete. We will also email or telephone you to ask some questions again 6 months and one year after your operation. These questions should take 10 minutes to answer. All of these questions are aimed at understanding how you feel about your general health and quality of life. This information will help us provide better information for future patients about what to expect from their surgery and how they will recover afterwards. If you later decide not to answer these questions, you do not have to.
To know the purpose(s) for the processing of their information.	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Why does PQIP need my personal details? To help PQIP provide an in-depth

			picture of your care, we send your personal details (NHS number, date of birth, postcode) to NHS Digital (England), NHS Wales Informatic Service (Patient Episode Database for Wales, Wales) or NHS National Services Scotland (Scotland). These organisations will link information to individual participants in the study which will tell us if you have (for example) been readmitted to hospital after you went home. In addition NHS Digital, NHS Wales Informatic Service, and National Services Scotland are able to provide us with information about people who may have passed away in order that we do not make contact and cause any distress to relatives. This information includes date and cause of death which is sourced from civil registration data on behalf of the Office for National Statistics. The linked information is

			returned to the PQIP study team in a digital file. The only identifiable details included in this file are your study ID and any information provided on the date and cause of death. The personal details (listed below) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else outside the NHS or research team. Personal details needed by PQIP are: ✓ Name ✓ Date of birth ✓ Postcode ✓ NHS number The information collected by PQIP is only used for research after it has been made anonymous. Who will be able to access my information? Your information will be anonymised before it is analysed by the study team. Your personal

			details (detailed above) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else outside the NHS or research team. Only doctors and approved researchers will be able to access the anonymised information which is collected through the PQIP study.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.			
The source of the data (where the data were not collected from the data subject)	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Why does PQIP need my personal details? To help PQIP provide an in-depth picture of your care, we send your personal details (NHS number, date of birth, postcode) to NHS Digital (England), NHS Wales Informatic Service (Patient Episode Database for Wales, Wales) or

			NHS National Services Scotland (Scotland). These organisations will link information to individual participants in the study which will tell us if you have (for example) been readmitted to hospital after you went home. In addition NHS Digital, NHS Wales Informatic Service, and National Services Scotland are able to provide us with information about people who may have passed away in order that we do not make contact and cause any distress to relatives. This information includes date and cause of death which is sourced from civil registration data on behalf of the Office for National Statistics. The linked information is returned to the PQIP study team in a digital file. The only identifiable details included in this file are your study ID and any information provided on the date and cause of death.

			The personal details (listed below) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else outside the NHS or research team. Personal details needed by PQIP are: ✓ Name ✓ Date of birth ✓ Postcode ✓ NHS number The information collected by PQIP is only used for research after it has been made anonymous.
Categories of data being processed	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Personal details needed by PQIP are: ✓ Name ✓ Date of birth ✓ Postcode ✓ NHS number
Recipients or categories of recipients	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	Who will be able to access my information? Your information will be anonymised before it is analysed by the study team. Your personal details (detailed above) are only shared with NHS Digital, NHS Wales Informatic Service (Patient Episode

			Database for Wales) or NHS National Services Scotland to enable the linkage to the information held by them. Your details will not be shared with anyone else outside the NHS or research team. Only doctors and approved researchers will be able to access the anonymised information which is collected through the PQIP study.
The source of the personal data	Included in Patient Information leaflet & website	Available on website - https://pqip.org.uk/pages/patients	
To know the period for which their data will be stored (or the criteria used to determine that period)			
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)			

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

?????

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- 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.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.

- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
You should include illegitimate access, undesired modification and disappearance of data								
Corporate risks & compliance risks section								

Regularly reviewing the DPIA

DPIA should be an ongoing process and regularly reviewed during the lifecycle of the project or programme to ensure

- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

You must add to your DPIA every time you make changes to the existing projects, send an updated version to your HQIP project manager and ensure that you incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

Appendix 1 Submitting your own version of DPIA

If submitting your own version of DPIA please ensure it includes the following items. If any items are missing please add this to your DPIA and then submit it. You must also complete the screening questions above.

	Checkbox – Please tick	Evidence – Page number and section in your DPIA
Confirmation of advice /consultation sought from Data Protection Officer whilst completing the DPIA		
Name of DPO		
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.		
Will the DPIA be published or part of it such as the summary or conclusion (not essential but encouraged). If so, where is it published?		
Does it include a systematic description of the proposed processing operation and its purpose?		
Does it include the nature, scope, context and purposes of the processing		
Does it include personal data, recipients and period for which the personal data will be stored are recorded		
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)		
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights		
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA		
Was consultation of the document carried out and with whom?		

Organisations ICO registration number		
Organisations ICO registration expiry date		
Version number of the DPIA you are submitting		
Date completed		

Appendix 2 Guidance for completing the table

<table>
<tr><td>What are the potential risks to the individuals whose personal data you hold?</td><td>See examples above</td></tr>
<tr><td>Likelihood of this happening (H,M,L)</td><td>
<table>
<tr><th>Likelihood score</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Very unlikely</td><td>May only occur in exceptional circumstances</td></tr>
<tr><td>2</td><td>Unlikely</td><td>Could occur at some time but unlikely</td></tr>
<tr><td>3</td><td>Possible</td><td>May occur at some time</td></tr>
<tr><td>4</td><td>Likely</td><td>Will probably occur / re-occur at some point</td></tr>
<tr><td>5</td><td>Very likely</td><td>Almost certain to occur / re-occur</td></tr>
</table>
</td></tr>
<tr><td>Impact (H,M,L)</td><td>
<table>
<tr><th>Impact scores</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Insignificant</td><td>No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality</td></tr>
<tr><td>2</td><td>Minor</td><td>Minor (<£100k) financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity, breach of confidentiality where < 20 records affected or risk assessed as low where data pseudonymised/files encrypted and no sensitive data</td></tr>
<tr><td>3</td><td>Moderate</td><td>Disruption to financial systems (<£250k); significant slippage in work activity or resources e.g. delay in recruiting staff; procedures and protocols require significant review, breach of confidentiality/ loss personal data where < 100 records involved and no sensitive data</td></tr>
<tr><td>4</td><td>Major</td><td>Major financial loss (£500k); large scale disruption to deliverables & project plans; business activity severely undermined, wasting considerable time / resources; poor quality report leading to loss of confidence in provider / HQIP / NHSE, breach of confidentiality/loss of personal sensitive data or up to 1000 records</td></tr>
</table>
</td></tr>
</table>

	5	Catastrophic	Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved
Risk score (calculated field)	Please multiply the likelihood by the severity (likelihood x severity = risk score). This score will help to rank the risk so the most severe risks are addressed first		
Will risk be accepted, reduced or eliminated? (where risk is accepted give justification)	A = Accepted (must give rationale/justification) R = Reduced E = Eliminated		
Mitigating action to reduce or eliminate each risk	Insert here any proposed solutions – see managing privacy and related risks section above OR If a risk has been accepted please give justification here (The purpose of the DPIA is to reduce the risk impact to an acceptable level while still allowing a useful project to be implemented.)		
Explain how this action eliminates or reduces the risk	Describe how your proposed action eliminates or reduces the possible risk. You may want to assess the costs/resource requirements (i.e. purchasing additional software to give greater control over data access and retention) and balance these against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.		
Expected completion date	What is the expected completion date for your proposed action? Ensure that DPIA actions are integrated into the project plan. You should continue to use the PIA throughout the project lifecycle when appropriate. The DPIA should be referred to if the project is reviewed or expanded in the future.		
Action Owner	Who is responsible for this action?		