Data Protection Impact Assessment for the

National Confidential Enquiry into Patient Outcome and Death (NCEPOD)

Document control:

	Name and role	Contact details
Document Completed by	Kirsty MacLean Steel Information Governance Lead	kmacleansteel@ncepod.org.uk
Document Updated by	Neil Smith Data Protection Officer	nsmith@ncepod.org.uk
DATA PROTECTION OFFICER	Neil Smith	nsmith@ncepod.org.uk
Document approved by (this should not be the same person that completes the form).	M. Ma	mmason@ncepod.org.uk
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5442652	

Date Completed	Version	Summary of changes
30/4/18	1	Completed first draft
31/1/19	1.1	
13/5/19	1.2	Reviewed and minor updates
06/02/20	1.3	Reviewed and minor updates
03/05/21	1.3	No changes needed
16/03/22	1.4	Reviewed and minor updates – data flow
22/05/23	1.5	Reviewed and minor updates – data flow
26/07/23	1.6	Data flow diagram replaced with link for ease of viewing

DATE OF NEXT REVIEW

31st March 2026

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		Healthcare records
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.	Yes		Studies may involve children and people with communication difficulties.
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		Not always but some studies involve match data from different services about the same patients.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	No		
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?	Yes		Compliance with the National Data Opt-Out means that NHS numbers will need to be checked against the spine

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.

The DPIA was updated in February 2020 as part of reaching compliance with the National Data Opt-Out therefore all NCEPOD studies were in various stages – with two holding patient identifiable data.

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

The aim of the project is to identify problems in clinical areas by reviewing case notes to assess the quality of the care provided. Healthcare providers identify patients meeting a set of criteria provided by us, a sample is selected from those patients and case notes and questionnaires are provided by the clinicians/hospitals, anonymised and reviewed.

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.

You 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.

The following groups are used as part of the DPIA consultation: Data Protection Officer| Information Security Forum| NCEPOD Clinical Team| NCEPOD Steering Group | NCEPOD Lay Representatives and ongoing consultation via the NCEPOD Local Reporters and Ambassadors. Contacting service users would not be possible as we do not have consent.

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.

Website – www.ncepod.org.uk

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.

DATA FLOW - https://www.ncepod.org.uk/pdf/current/Data%20flow%202024.pdf

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).

NA

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 individuals*]	**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		For case note reviewers only, for communication purposes.
Address	Yes		For case note reviewers only, for communication purposes.
Postcode	Yes		For case note reviewers only, for communication purposes.
Patient – study data			
NHS number	Yes		This is used so that we can collect the correct case notes after a random sample has been selected.
Date of birth	Yes		This is only collected when age is needed, such as where a specific age group is relevant.
Date of death	Yes		Only collected if necessary, such as looking at deaths within a certain time of intervention, discharge etc.
Age	No		

Data Categories [*Information relating to the individuals*]	**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]*
Sex	Yes		In some cases, it is necessary to look at male and female populations separately and this will be collected under staff information
Marital Status	Yes		This will be collected under staff information
Gender	No		
Living Habits	No		
Professional Training / Awards	Yes		Case reviewers and this will be collected under staff information
Income / Financial / Tax Situation	No		
Email Address	Yes		For case note reviewers only, for communication purposes.
Physical Description	No		
General Identifier e.g. Hospital No	Yes		NHS number is not always available and there needs to be a means of ensuring that the correct patient is included.
Home Phone Number	Yes		For case note reviewers only, for communication purposes and staff
Online Identifier e.g. IP Address/Event Logs	No		
Website Cookies	No		
Mobile Phone / Device No	Yes		For case note reviewers only, for communication purposes and staff
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	Yes		We collect information on people with specific health conditions, which differ between each study. To ensure we get the right sample we collect information on diagnosis. We then collect health records relating to that condition to be reviewed.
Sexual Life / Orientation	No		
Family / Lifestyle / Social Circumstance	No		
Offences Committed / Alleged to have Committed	No		
Criminal Proceedings / Outcomes / Sentence	No		
Education / Professional Training	Yes		For case note reviewers only, for communication purposes and staff

Data Categories [*Information relating to the individuals*]	**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]*
Employment / Career History	Yes		For case reviewer selection and staff
Financial Affairs	No		
Religion or Other Beliefs	No		
Trade Union membership	No		
Racial / Ethnic Origin	Yes		For staff this is recorded for equality purposes and for studies it is used for healthcare inequalities assessments
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 ask healthcare providers for specific information, usually NHS number, date of birth, admission and/or discharge dates, ICD-10 or OPCS codes. We use criteria for identifying the correct patients, such as clinical codes, time period of admission. Information is then provided by the healthcare provider from their information system. These are unlikely to change but if contradictory information is provided this will be checked with the healthcare provider and updated on our database. All studies are for a fixed period (usually 2 years) and personal data is not kept beyond the end of the study.

Personal data relating to case note reviewers (name, address and email) is kept in a spreadsheet on a part of the network only accessible by non-clinical NCEPOD staff.

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
Individuals are clear about how their personal data is being used.	Privacy notice Patient leaflet Information given to healthcare providers	These are available on the website and sent to all healthcare providers for each study.
Individuals can access information held about them	Information on our website and link for people to contact us. Patient leaflet	These will be available on the website and sent to all healthcare providers for each study. Primary advice is that service users should contact their healthcare provider if they want to obtain a copy of their notes.
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	Information on our website and link for people to contact us if they want to opt out of any or all NCEPOD studies. Patient leaflet Need to ensure it's clear that this is just for NCEPOD. – study by study basis	These will be available on the website and sent to all healthcare providers for each study.
Rectification of inaccurate information	Data subjects would need to correct information through their healthcare provider.	
Restriction of some processing	Patient leaflet, information on our website and link for people to contact us if they want to restrict processing of their data. We will make it clear that restriction of data will be treated as erasure and the subject will be removed from our records entirely.	These will be available on the website and sent to all healthcare providers for each study.

Object to processing undertaken on some legal bases	Information on our website and link for people to contact us if they want to object to the processing of their data. We will make it clear that objection will be treated as erasure and the subject will be removed from our records entirely.	These will be available on the website and sent to all healthcare providers for each study.
Complain to the Information Commissioner's Office;	Information and link on our website	
Withdraw consent at any time (if processing is based on consent)	Our processing is not based on consent.	
Data portability (if relevant)	Personal data is not transferred or reused in any way.	
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Information and link on our website	These will be available on the website and sent to all healthcare providers for each study.
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.	In privacy notice Information and link on our website	These will be available on the website and sent to all healthcare providers for each study.
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?	Privacy notice Patient leaflet Information given to healthcare providers	These will be available on the website and sent to all healthcare providers for each study.
To know the purpose(s) for the processing of their information.	Privacy notice Patient leaflet Information given to healthcare providers	These will be available on the website and sent to all healthcare providers for each study.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Privacy notice Patient leaflet Information given to healthcare providers	These will be available on the website and sent to all healthcare providers for each study.
The source of the data (where the data were not collected from the data subject)	Privacy notice Patient leaflet Information given to healthcare providers	These will be available on the website and sent to all healthcare providers for each study.
Categories of data being processed	Patient leaflet Information given to healthcare providers	These will be available on the website and sent to all healthcare providers for each study.

	Information on our website	
Recipients or categories of recipients	Patient leaflet Information given to healthcare providers Information on our website	These will be available on the website and sent to all healthcare providers for each study.
The source of the personal data	Patient leaflet Information given to healthcare providers Information on our website	These will be available on the website and sent to all healthcare providers for each study.
To know the period for which their data will be stored (or the criteria used to determine that period)	Patient leaflet Information given to healthcare providers Information on our website	These will be available on the website and sent to all healthcare providers for each study.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	Not 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 regard 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.

> The number of individuals depends on how many studies are running and the patient population. If three studies are collecting data in a year the data could be collected on approximately 45,000 people. This would be the initial data collection before sample selection takes place which would be in the region of 3000 people.

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 more 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**
Access to files by someone without permission	1	1	1	**Reduced**	Security measures in the office. File cupboard closed and locked when there is a possibility of access.	Reduces opportunity for files to be accessed.	Ongoing	Data Protection Officer
Loss of data	1	2	2	**Eliminated**	Security measures. No personal identifiable data removed from office.	Reduces opportunity for data to be lost.	Ongoing	Data Protection Officer
Recognition of individuals	1	2	2	**Eliminated**	No patient identifiable data used in reports. Case scenarios used composite data or themes rather than individual cases.	No individual data made available.	Ongoing	Data Protection Officer
Identifiable data seen by people without permission, such as case note reviewers	1	2	2	**Eliminated**	All patient identifiable data is removed or anonymised	Removes identifiable information before case note review.	Ongoing	Data Protection Officer
IT security breach	1	4	4	**Reduced**	Security measures e.g. firewall, passwords. Documents password-protected when emailing.	Reduces opportunity for access to files.	Ongoing	Data Protection Officer

What are the potential risks to the individuals whose personal data you hold?	Likelihood of this happening	Impact	Overall risk 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
Loss of information en route from healthcare provider to NCEPOD	1	4	4	Reduced	Secure, addressed plastic envelopes are provided with questionnaires. Healthcare providers are encouraged to send case notes, spreadsheets and questionnaires password-protected electronically through the NHS net.	Plastic envelopes are more secure than paper ones which can tear easily, especially is large amounts of papers are included. Emailing information through the NHS network is more secure than sending physical copies. All documents are required to be password-protected so can't be opened without a password.	Ongoing	Data Protection Officer
What are the potential corporate risks & compliance risks?	**Likelihood of this happening**	**Impact**	**Overall risk 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**
Non-compliance with policies and protocols	1	2	2	Reduced	Policy and procedures in place, reviewed and monitored regularly.	Problems can be identified and rectified	Ongoing	Data Protection Officer

Receipt of data outside of time period and criteria	4	1	4	**Reduced**	Add to data breach spreadsheet Contact healthcare provider Destroy data	Inappropriate data is not used in analysis or kept in office Providers are reminded to use criteria and not send inappropriate data	Ongoing	Data Protection Officer
Reputational damage	1	4	4	**Reduced**	Security measures in place All patient identifiable data is removed or anonymised	Reduces likelihood of a problem occurring	Ongoing	Data Protection Officer
Financial costs	1	4	4	**Reduced**	Security measures in place All patient identifiable data is removed or anonymised	Avoiding data security problems negates any financial penalties	Ongoing	Data Protection Officer

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.

Appendix 2 Guidance for completing the table

What are the potential risks to the individuals whose personal data you hold?	See examples above		
Likelihood of this happening (H,M,L)	**Likelihood score**	**Description**	**Example**
	1	Very unlikely	May only occur in exceptional circumstances
	2	Unlikely	Could occur at some time but unlikely
	3	Possible	May occur at some time
	4	Likely	Will probably occur / re-occur at some point
	5	Very likely	Almost certain to occur / re-occur
Impact (H,M,L)	**Impact scores**	**Description**	**Example**
	1	Insignificant	No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality
	2	Minor	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
	3	Moderate	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

<table>
<tr><td></td><td><table>
<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>
<tr><td>5</td><td>Catastrophic</td><td>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</td></tr>
</table></td></tr>
<tr><td><b>Risk score (calculated field)</b></td><td>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</td></tr>
<tr><td><b>Will risk be accepted, reduced or eliminated?</b> (where risk is accepted give justification)</td><td>A = Accepted (must give rationale/justification)
R = Reduced
E = Eliminated</td></tr>
<tr><td><b>Mitigating action to reduce or eliminate each risk</b></td><td>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.)</td></tr>
<tr><td><b>Explain how this action eliminates or reduces the risk</b></td><td>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.</td></tr>
<tr><td><b>Expected completion date</b></td><td>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.</td></tr>
<tr><td><b>Action Owner</b></td><td>Who is responsible for this action?</td></tr>
</table>