Data Protection Impact Assessment for NEIA Audit

Document control:

	Name and role	Contact details
Document Completed by	**Sarah Gallagher, Clinical Audit Project Manager**	+44 (0)20 7842 0900
Data Protection Officer name	**Caroline Wilson, Head of Operations and HR, Data Protection Officer**	+44 (0)20 7842 0900
Document approved by (this should not be the same person that completes the form).	**Neena Garnavos, Head of Quality Improvement**	+44 (0)20 7842 0900
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z127452X**	

Date Completed	Version	Summary of changes
12/04/2018	1.1	Updates
18/07/18	1.2	Updates
30/11/18	1.3	Updates
21/05/19	1.4	Updates
30/02/20	1.5	Updates
10/09/20	1.6	Updates
22/08/21	1.7	Updates
28/04/22	1.8	Updates
01/02/24	1.9	Updates

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		
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		
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		Hospital Episode Statistics (HES) data from NHS Digital, mortality data from ONS, The Patient Episode Database for Wales
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?	No		This is an existing project which has been recommissioned with an extended scope.

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.

During the implementation phase

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

The National Early Inflammatory Arthritis Audit (NEIAA) aims to improve the quality of care for patients with early inflammatory arthritis in England and Wales, by assessing rheumatology units against key performance measures such as waiting time, time to treatment, outcome measures and clinical responses. The scope of the audit has now been extended to include data collection on rarer IMIDs for referral and diagnosis.

Below is a summary of the information being collected in the audit. Data is inputted by clinicians in rheumatology departments via a secure online portal and patients input the PROMs data outlined below via another portal:

Core patient identifiers: Name, Date of Birth, NHS number, hospital number, full postcode, email address.
Demographics: gender, ethnicity, smoking status, work status.
Baseline: primary diagnosis, comorbidity, disease severity measure, treatments.
3 month: disease severity measure, treatments.
PROMS at baseline, 3 month, 6 month, 9 month and 12 month: MSKHQ, HAQ2, GAD2 PHQ2, WPAI.
Data Linkage: HES, PEDW, ONS.

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.

There was a wide consultation regarding the data protection implications of the audit, partly to satisfy the information governance requirements in our contract and in relation to our application to the Health Research Authority for exemption to written consent. Below is a list of the groups that have informed this:

Senior Governance Group – the main board for this project made up of representatives external to the core project such as patient charities, HQIP, research funders etc. They reviewed our IG policies and documents.

Patient and Public Involvement Panel – established to provide expert patient advice on the development of the audit. They informed the development of our patient information leaflet and privacy notice.

Project Working Group – core advisory group on development and delivery of audit. They advised on many aspects of data protection including the consent model and application to HRA.

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.

A summary of Data Protection Impact Assessment is published on the main audit website www.arthritisaudit.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 being collected for audit
Clinicians will input data in rheumatology departments via a secure online portal and patients who will input PROMS via the patient portal. Below are the key data items that will be collected:

Core patient identifiers: Name, Date of Birth, NHS number, hospital number, full postcode, email address, telephone number.
Demographics: gender, ethnicity, smoking status, work status.
Baseline: primary diagnosis, comorbidity, disease severity measure, treatments.
3 months: disease severity measure, treatments.
PROMS at baseline, 3 months, 6 months, 9 months and 12 months: MSKHQ, HAQ2, GAD2 PHQ2, WPAI.

Data processors
Net Solving and KCL will be the primary data processors for the audit. Both are experienced in data processing for large scale national projects. Net solving, as the IT company commissioned to manage the online data portal, will be the primary data processors including identifiable information for the purposes of linkage. King's College London academic rheumatology unit will receive data, pseudonymised by Netsolving, for the purpose of audit analysis and reporting

Data linkage
To satisfy our contractual requirements, we link to the following databases:

- **Death Register held by the Office for National Statistics (ONS)**. The data will provide validated mortality information in England and Wales
- **HES admitted patient data** http://www.hscic.gov.uk/hesdatadictionary and **PEDW admitted patient data** (for Wales) http://www.datadictionary.wales.nhs.uk/. The linkage with HES / PEDW will enable us to calculate the rate of emergency hospitalisations, and joint replacement surgeries.

The linkage of audit data to HES will be performed by NHS Digital. To avoid the transmission of patient medical information, only demographic identifiers (date of birth, NHS number, postcode) are passed to NHS digital. They then provide a pseudonymised unique 32-character alphanumeric field patient identifiers (HESID) of the patients in the audit. A similar process is employed to link with PEDW.

Data Safeguards
The following measures are in place to safeguard the security of the data:

- Clinicians will have unique logins. They will only see data for their own patients.
- The web audit tool will be hosted by Rackspace, a leading web hosting provider.
- The data will be stored in a Microsoft SQL Server database, secured using Windows Authentication which prevents login information being stored in the application.
- Net Solving will host an SQL database in a RAID array preventing data loss if a hard drive fails.
- Data will be backed up in a secure remote physical location.
- KCL will access pseudonymised data directly from the web portal.
- KCL will adhere to institutional data handling policies, accredited by the HTA for clinical trial conduct, and recently audited by the MHRA.

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).

No personal data will be transferred outside the EEA

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		Allows hospitals to easily locate individual's forms
NHS number	Yes		Linkage to HES data on hospitalisations, joint replacements, and deaths.
Address	No		
Postcode	No		Linkage to IMD deprivation data for case-mix adjustment. Additional identifier to support deterministic matching with HES.
Date of birth	Yes		Case-mix adjustment. To allow fairer comparisons between services that serve sociodemographically distinct populations. Additional identifier to support deterministic matching with HES.
Date of death	No		
Age	No		Case-mix adjustment. To allow fairer comparisons between services that serve sociodemographically distinct populations. Additional identifier to support deterministic matching with HES.
Sex	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]*
Marital Status	No		
Gender	Yes		Case-mix adjustment. To allow fairer comparisons between services that serve sociodemographically distinct populations. Additional identifier to support deterministic matching with HES.
Living Habits	No		
Professional Training / Awards	No		
Income / Financial / Tax Situation	No		
Email Address	Yes		To allow contact for patient reported outcome form completion.
Physical Description	No		
General Identifier e.g., Hospital No	Yes		Unique identifier for hospital level data linkage across baseline and follow up forms.
Home Phone Number	Yes		Only if offered by patient to allow contact for patient reported outcome form completion if they are unable to access the internet.
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	Yes		Assessment of disease impact
Sexual Life / Orientation	No		
Family / Lifestyle / Social	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]*
Circumstance			
Offences Committed / Alleged to have Committed	No		
Criminal Proceedings / Outcomes / Sentence	No		
Education / Professional Training	No		
Employment / Career History	Yes		Assessment of disease impact on capacity to work.
Financial Affairs	No		
Religion or Other Beliefs	No		
Trade Union membership	No		
Racial / Ethnic Origin	Yes		Equality of care: to evaluate if there is differential access to EIA services. Case-mix adjustment. To allow fairer comparisons between services that serve sociodemographically distinct populations.
Biometric Data (Fingerprints / Facial Recognition)	No		
Genetic Data	No		
Smoking status	Yes		Case-mix adjustment. To allow fairer comparisons between Trusts that serve sociodemographically distinct populations.
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.

The IT platform for data collection will include automatic data verification processes (e.g. NHS number data field requirements of numeric ten digits in 3-3-4 format). The platform will allow clinicians to update data fields where necessary.

For the purpose of linkage multiple identifiers will be used for deterministic matching with NHS digital (date of birth, NHS number, postcode) to ensure data accuracy.

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	Published on audit website	The confidential information we are collecting is your name, email address, date of birth, NHS number, postcode and gender. The benefit of gathering these personal details is to enable the NEIAA project team to link with other sources of information within the NHS to learn about the impact on patients of inflammatory arthritis and its treatments.
Individuals can access information held about them	Included in the privacy notice	Published on audit website	If you would like to see your information, please contact your local Rheumatology department
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 the privacy notice and patient information leaflet	Published on the audit website	Please contact your rheumatology department and inform them that you do not wish your data to be included. They will then contact BSR with your Case ID and we will remove your record from the audit.
Rectification of inaccurate information	In FAQs	Published on the audit website	If you have submitted incorrect information, please contact your rheumatology department in order to change this.
Restriction of some processing			
Object to processing undertaken on some legal bases			
Complain to the Information Commissioner's Office	Included in the patient information leaflet and privacy notice	Published on audit website	You also have the right to raise concerns or make a complaint through the Information

			Commissioners Office by calling 0303 123 1113 or following the link https://ico.org.uk/concerns/.
Withdraw consent at any time (if processing is based on consent)			Data processing is not based on consent.
Data portability (if relevant)			Not relevant – patients can view their own entered data but not download it or print it.
Individual knows the identity and contact details of the data controller and the data controller's data protection officer	Included in the privacy notice	Published on the audit website	The joint data controllers are HQIP, NHS England and the Welsh government. You can contact HQIP's data protection officer at data.protection@hqip.org.uk. The BSR's data protection officer is Caroline Wilson, and can be contacted on cwilson@rheumatology.org.uk
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 the privacy notice	Published on audit website	No personal information will ever be made public, and no data will be transferred outside of the EU.
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 the privacy notice	Published on the audit website	The legal basis for processing the information collected is article 9 (2) (i) of GDPR 'processing is necessary for reasons of public interest in the area of public health'
To know the purpose(s) for the processing of their information	Included in the patient information leaflet and privacy notice	Published on the audit website	We hope that by gathering information directly from you we will get more accurate information and we will help patients to feel empowered to communicate more with their clinicians, their families and employers and manage their

			disease more effectively day to day. The purpose of the NEIAA is to improve the quality of care for patients with inflammatory arthritis. The audit will assess care provided to people with new symptoms of arthritis attending rheumatology services for the first time. The benefit of gathering these personal details is to enable the NEIAA project team to link with other sources of information within the NHS to learn about the impact on patients of inflammatory arthritis and its treatments.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data			Not relevant
The source of the data (where the data were not collected from the data subject)	Included in the privacy notice and data flow map	Audit website	HES, PEDW, ONS mortality and Index of Multiple Deprivation (IMD) rank
Categories of data being processed	Included in the privacy notice and data flow map	Audit website	Identifiable, pseudonymised, anonymised and aggregated
Recipients or categories of recipients	Included in the privacy notice	Audit website	Data from the audit may also be shared to third party applicants for the purposes of research, service evaluation and health/care improvement. Sharing data will always be under relevant legal and information governance regulations.
The source of the personal data	Included in the patient information leaflet and privacy notice	Published on the audit website	Information will be collected from the team you see in clinic. Members of your rheumatology team will complete questions about your condition.

To know the period for which their data will be stored (or the criteria used to determine that period)	Included in the privacy notice	Published on the audit website and in patient information sheet	We will store your data in an identifiable format for 10 years and after that time it will be de-identified.
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 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.

The project currently holds almost 73,000 patient records. Over 10,000 patients have been recruited each year excluding during the pandemic (April 2020-March 2021).

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**
Data loss or inappropriate disclosure of patient identifiable data	2	4	8	**Reduced**	Strict adherence to security and governance protocols and working to highest information governance standards. This includes robust contract management with Netsolving and KCL and Training and awareness for staff. Secure audit data portal and minimising number of parties with access to identifiable data.	These measures ensure that the likelihood of this risk occurring is reduced as the data is held securely	March 2018	PM
Data breach through downloading of data in an insecure location	2	3	6	**Reduced**	On the website we state very clearly that once the data has been downloaded it is the responsibility of the user. We also only allow site	Users will be more aware once they see our warning that the data is their responsibility if they	May 2018	PM

					administrators to download data from the NEIAA.	download it and should be more considerate about what they do with the data. As all users are NHS staff, they should already have training in patient confidentiality and data protection. By limiting the number of users who can download data we reduce the risk of data being downloaded unnecessarily.		
Risks during data transfer	1	2	2	**Reduced**	Data will be transferred securely, using encryption and password protection on sensitive files.	These steps will ensure that sensitive files are protected.	February 2019	PM
Failure to respond appropriately to data breach	1	3	3	**Reduced**	In case of data breach, we will immediately notify HQIP and seek advice from Net Solving and other experts as to how to deal with the breach.	Communicating with the relevant personnel will allow us to adequately deal with any issues that arise.	February 2019	PM
Trusts fail to comply with the national opt-out	2	3	6	**Reduced**	Instructions on the requirements for compliance with the national opt-out are outlined on the page where site users upload their data. Also, guidance is available on the audit website, and	Trusts have the relevant information on the steps that they need to take to be compliant.	September 2021	PM

					information on compliance is included in the quarterly newsletter.			
Corporate risks & compliance risks section								
Failure to comply with national opt out	1	4	4	**Eliminated**	We have implemented the technical solution to ensure compliance with the national opt-out.	This action eliminates the risk as the system is in place.	September 2021	PM

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</td></tr>
</table>
</td></tr>
</table>

			confidentiality/loss of personal sensitive data or up to 1000 records
	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?