Data Protection Impact Assessment for

National Lung Cancer Audit (NLCA)

Document control:

	Name and role	Contact details
Document Completed by	**Neena Garnavos**	**Neena.garnavos@rcplondon.ac.uk**
Data Protection Officer name	**Pamela Forde**	**Pamela.forde@rcplondon.ac.uk**
Document approved by (this should not be the same person that completes the form).	**Teena Chowdhury**	**Teena.chowdhury@rcplondon.ac.uk**
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z7085833**	

Date Completed	Version	Summary of changes
16 May 2018	**V1.0**	

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?	Yes		NCRAS and WAG extract data that fit the NLCA dataset.
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		It is an essential requirement of PHE to process confidential patient information needed to register cancer cases. Approval to do this is gained via the section 251 application and approval process. This data is then pseudonymised and transferred to our other sub-contractor, UoN, to analyse the incidence, prevalence, treatment and outcomes of lung cancer. WAG
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		Trusts submit data for all lung cancer patients' diagnoses and/or treated in NHS trusts in England and Wales. This may include vulnerable

				individuals.
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		National Cancer Registration & Analysis Service (NCRAS)(PHE) extract, link and pseudonymise data before sending it to University of Nottingham (UoN) for analysis. Data is linked to ONS, HES, RTDS & SACT. WAG
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 lawful basis upon which National Cancer Registration and Analysis Service (NCRAS) / Public Health England (PHE) processes personal data is GDPR article 6(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

				This task is set out in UK law under the Heath Service (Control of Patient Information) Regulations 2002, which make provisions for confidential patient information in England and Wales to be processed without consent for medical purposes, where seeking consent is not practical and there is no practical alternative. The NCRAS/PHE processes health data in compliance with the conditions set out in GDPR article 9(2)(i) "processing is necessary for reasons of public interest in the area of public health such as … ensuring high standards of quality and safety of health care… on the basis of [UK] law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional

				secrecy. ” NCRAS provide pseudonymised data to NCLA. WAG
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		

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.

At the commencement of the 2 year contract extension.

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

The overall aim of the National Lung Cancer Audit (NLCA) is to drive further improvements in lung cancer care and outcomes by bringing the standard of all lung cancers teams up to that of that of the best. This audit was planned to evaluate the process of care, treatment delivered and outcomes for lung cancer patients treated in secondary/tertiary care NHS hospitals in England and Wales. We intended that all eligible providers would participate. We planned to audit a combination of process and outcome measures which are closely aligned to the NICE quality standards (QS) 2012, NICE lung cancer guideline 2011 (GL) and NICE technology appraisals (TA). Trusts submit data via the Cancer Outcomes Services Dataset (COSD) to the National Cancer Registration and Analysis Service (NCRAS). NCRAS load data from COSD into the English National Online Cancer Registration Environment (EnCORE) and the Cancer Access System (CAS), and then extract NLCA data from CAS. Data for surgical cohort are extracted and sent back to trusts to review and return to NCRAS. NCRAS link the data extract for NLCA with HES (Hospital Episode Statistics), ONS (mortality data), SACT (Systemic Anti-Cancer Therapy), and RTDS (Radiotherapy Dataset). NCRAS pseudonymise data extract and release to the University of Nottingham (UoN) for analysis via the Office for Data Release (ODR). WAG The sensitive data is analysed and prepared by UoN are released in an anonymised and aggregated form for NLCA to publish.

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.

Project management team, Data Protection Officer, senior management, other necessary audit and accreditation staff, sub-contractors for data processing and analysis.

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.

There is currently no plan to publish RCP DPIAs unless specific audit programmes are instructed by HQIP to do so.

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.

The NLCA data flow charts can be found below.

NCLA Data Flows.pdf

England

Stage 1 (data extraction): COSD data submitted by trusts is loaded into ENCORE by NCRAS. NCRAS transfer data into CAS and extract NLCA data from CAS.

Stage 2 (data linkage): Data are linked to HES, ONS, RTDS & SACT.

Stage 3 (data analysis): Pseudonymised data are release by ORD to the UoN for analysis.

Stage 4 (reporting): Anonymised and aggregated data are released to Royal College of Physicians for commentary and national and local reporting.

Wales

Stage 1 (data extraction): WAG send pseudonymised Patient Episode Database for Wales (PEW) to UoN.

Stage 2 (reporting): Anonymised and aggregated data are released to Royal College of Physicians for commentary and national and local reporting.

WAG have confirmed their data flow varied from PHE but have not yet released the data flow to RCP.

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).

No personal data is transferred outside of the EEA.

Privacy Risk Register

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		N/A	
NHS number	Yes		Enables linkage with external national datasets for case ascertainment and exploration of patient outcomes (readmissions and mortality). Also ensures checks can be carried out to make sure the correct patient has been entered. NHS number, postcode and data of birth are used for triangulation. It enables the NCRAS team to check, if an error has occurred, that the correct patient has been used for linkage etc. Multiple identifiers makes this easier and quicker.
Address		N/A	
Postcode	Yes		As above and also enables exploration of social and economic deprivation (using Index of Multiple Deprivation (IMD) and Welsh Index of Multiple Deprivation (WIMD). NHS number, postcode and data of birth are used for triangulation. It enables the NCRAS team to check, if an error has occurred, that the correct patient has been used for linkage etc. Multiple identifiers makes this easier and quicker.
Date of birth	Yes		As above and also enables exploration of equity of care. NHS number, postcode and data of birth are used for triangulation. It enables the NCRAS team to check, if an error has occurred, that the correct patient has been used for linkage etc. Multiple identifiers makes this easier and quicker.
Date of death		N/A	
Age		N/A	
Sex	Yes		As above and also enables exploration of social and economic deprivation (treatment and outcome of different genders), as well as equity of care.
Marital Status		N/A	
Gender	Yes		See sex.
Living Habits	Yes		Information on smoking are collected.
Professional Training / Awards		N/A	
Income / Financial / Tax Situation		N/A	

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]*
Email Address		N/A	
Physical Description		N/A	
General Identifier e.g. Hospital No		N/A	
Home Phone Number		N/A	
Online Identifier e.g. IP Address/Event Logs		N/A	
Website Cookies		N/A	
Mobile Phone / Device No		N/A	
Device Mobile Phone / Device IMEI No		N/A	
Location Data (Travel / GPS / GSM Data)		N/A	
Device MAC Address (Wireless Network Interface)		N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Clinical details of cancer diagnosis need for the audit.
Sexual Life / Orientation		N/A	
Family / Lifestyle / Social Circumstance		N/A	
Offences Committed / Alleged to have Committed		N/A	
Criminal Proceedings / Outcomes / Sentence		N/A	
Education / Professional Training		N/A	
Employment / Career History		N/A	
Financial Affairs		N/A	
Religion or Other Beliefs		N/A	
Trade Union membership		N/A	
Racial / Ethnic Origin	Yes		Enables assessment of equity of care across race and ethnic origin.
Biometric Data (Fingerprints / Facial Recognition)		N/A	
Genetic Data		N/A	

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.

NCRAS have a process for validation, which is set out later in this document.

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.	Personal data is collected as part of the Cancer register and NLCA only report on analysis conducted on pseudonymised data. PHE have section 251 approval for data processing. Information requested from WAG but not yet returned.		
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			
Rectification of inaccurate information			
Restriction of some processing			
Object to processing undertaken on some legal bases			
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			
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.			
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?			
To know the purpose(s) for the processing of their information.			
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)			
Categories of data being processed			
Recipients or categories of recipients			
The source of the personal data			
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.

All lung cancer patients diagnosed and/or treated in NHS hospital Trusts in England and Wales are included in this audit. We report on data from between 35000 to 40000 people 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**
Illegitimate access	1	5	5	**Reduced**	In accordance with the Data Protection Act (and forthcoming EU General Data Protection Regulation) and Caldicott principles, the PHE cancer registration service does take steps to limit its processing of confidential patient information. Since 2013, all the PHE cancer registration offices have been using the single English National Online Cancer Registration Environment (EnCORE) and the tied, but functionally discrete, Cancer Analysis System			

					(CAS). EnCORE and CAS provide a secure, role-based separation between the essential requirement to process the confidential patient information needed to register cancer cases, and the pseudonymised data that is needed to analyse cancer incidence, prevalence, treatment and outcomes. Role-based access controls are in place for CAS to ensure that authorised users can only see the data they need to do their job. There are three levels of access, with increasingly rigorous approval processes. First level users of the system can see record-level diagnosis and treatment data and partial dates (such as month and year but not day) but are not able to access names, addresses, NHS Numbers			

					and postcodes. Second level users are provided with access to the minimum number of patient identifiers needed for linkage purposes – such as NHS Number, date of birth and postcode – but cannot view other direct identifiers such as names and street addresses. Finally, third level users are provided with full access to all the patient identifiers recorded in the cancer registration data set but these requests are reviewed by NCRAS senior managers and only granted for analyses that depend on the complex matching of patient records. In summary, cancer registration in England fundamentally depends on the ability of PHE to process confidential patient information. But while it is not practicable			

					or proportionate to obtain consent or to work with anonymised data only, the National Cancer Registration and Analysis Service does take steps to limit the processing of confidential data to ensure compliance with data protection legislation and the Caldicott principles. WAG			
Undesired modification	1	4	4	**Reduce**	As above WAG			
Disappearance of data	1	5	5	**Reduce**	PHE			
Sub-contractor data breach	3	3	9	**Reduce**	Robust sub-contract in place with University of Nottingham to ensure level of data is secure and non-transferable. Ensure contract with Nottingham is reviewed and updated before expiry.			
RCP Network Failure or cyber attack	3	2	6	**Eliminate**	Alternative download options are available; logging and learning from previous issues encountered; allowing lead/lag times in reporting analysis periods to allow for delays.			
Corporate risks & compliance risks section								

Loss of clinical 'buy in'	3	4	12	**Reduce**	Risk is minimised by producing timely bespoke reports at agreed intervals, ensuring data transparency is maintained; frequent and effective communications with stakeholders; operating a knowledgeable inbox; producing supporting information to assist in data interpretation, hosting events, user groups, conferences for clinical teams to attend; improving the accessibility of the data and providing examples of QI, celebrating and sharing success with clinical users - research papers; sharing good practice with case studies. Involve clinical director in decisions and comms when appropriate.			
Reporting Errors	4	3	12	**Reduce**	NLCA data is extensively QA'd from receiving raw data, through to report production, checking, sign off, and dissemination. Data are shared with lung cancer clinical leads/surgical leads for checking prior to publication. Potential issues escalated to senior managers when identified.			
Maintaining Data Quality	3	2	6	**Reduce**	The NLCA now receives cancer registry data for England. This includes additional datasets and combined we are confident we receive high quality data			

					on all lung cancers. Data completeness is an issue in some areas and Public Health England team have a team of staff working regionally to improve data completeness. Data completeness reports are produced monthly and circulated to trusts			
Contracts and Licences Expiry	2	5	10	**Reduce**	Risk is minimised by devising and updating a centrally stored timetable, which is regularly reviewed across CQID for shared experience. We have a schedule of all timelines which includes details about who actions each element			

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 colspan="3">See examples above</td></tr>
<tr><td>Likelihood of this happening (H,M,L)</td><td colspan="3"><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 colspan="3"><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?