Data Protection Impact Assessment for the National Paediatric Diabetes Audit

Document control:

	Name and role	Contact details
Document Completed by	Amani Krayem, NPDA Project Manager	Amani.krayem@rcpch.ac.uk 020 7092 6157
Data Protection Officer name	Head of Information Governance	information.governance@rcpch.ac.uk 020 7092 6000
Document approved by (this should not be the same person that completes the form).	Head of Information Governance	information.governance@rcpch.ac.uk 020 7092 6000
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5143673	

Date Completed	Version	Summary of changes
27/04/2018	**1**	
15/05/2018	**3.1**	**IGM/DPO comments and amendments**
21/09/2018	**3.2**	**HR further amends following comments from HQIP**
01/10/2018	**3.3**	**IGM further amends**
26/07/2019	**3.4**	**Further IGM following response to comments by project lead**
14/08/2019	**3.7**	**Final comments by HR**
16/08/2020	**3.8**	**Approved version**
17/07/2023	**3.10**	**Review- minor amendments**
21/06/2024	**3.11**	**Inclusion of Jersey and Hybrid Closed Loop Data Provision Notice**
21/02/2025	**3.12**	**Minor amendments to reflect changes to the NPDA data collection system**
09/04/2025	**3.13**	**Updated mitigating actions in the risks table.**
13/10/2025	**3.14**	**Updated subprocessors**

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?	N		
2	Does your project involve any sensitive information or information of a highly personal nature?	Y		
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.	Y		
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?	N		
5.	Does your project match data or combine datasets from different sources?	N		Historically we have linked data to HES and PEDW data provided by NHS England and the DHCW (previously 'NHS Wales Informatics Service') (previous PIA v3.8). There are no further plans for this or other linkage by the NPDA team.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	N		

7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	N		
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?	N		

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.

Retrospectively

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

The report aims to address a series of questions relating to paediatric diabetes care, which include: • What proportion of children and young people with diabetes are reported to be receiving key age-specific processes of diabetes care, as recommended by NICE? • How many achieve outcome measures within specified treatment targets? • Are children and young people with diabetes demonstrating evidence of small vessel disease (microvascular) and/or abnormal risk factors associated with large vessel disease (macrovascular) prior to transition into adult services?

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 privacy leaflet has been developed with the RCPCH Data Protection Officer June 2024. This updates the previous privacy notice to include the collection of patient identifiable information from paediatric diabetes units within Jersey as well as to include the HCL data sharing.

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.

We will publish this on the NPDA webpages.

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.

Processing activity description	Type of data involved	Data flow	Controller/processor
Submission of NPDA dataset by paediatric diabetes units	Personal data (identifiable)	From paediatric diabetes units to the NPDA data collection platform Occasional submission by units outside of submission window via RCPCH SharePoint m365.	Data controllers: Paediatric diabetes units Processor: NPDA Subprocessors: Microsoft, SysGroup
Download and validation of NPDA data extracted from submission platform	Personal data (identifiable)	From the secure platform database to NPDA (SharePoint m365 and onsite servers manged by RCPCH)	Joint Controllers: HQIP and NHS England Processor: NPDA, Sub-processor: Microsoft, SysGroup
Data cleaning and preparation of data for analysis-	Personal data (identifiable)	-	Joint Controllers: HQIP and NHS England Processor: NPDA
Production of unit/regional network, NHSE region, ICS national level results	Aggregated	-	Joint Controllers: HQIP and NHS England Processor: NPDA
Submission of service level data including some patient characteristics	Aggregated	-	Joint Controllers: HQIP and NHS England Processor: NPDA
Cleaning, analysis, and reporting of spotlight audit data	Aggregated (spotlight audit collects unit level data only)	-	Joint Controllers: HQIP and NHS England Processor: NPDA
Parent and patients submit views on care via online PREM surveys	Anonymised	Parents and Patients to online submission portal: SurveyMonkey Enterprise managed by RCPCH	Joint Controllers: HQIP and NHS England Data sub processor: SurveyMonkey Data processor: NPDA
Cleaning and analysis of PREM data	Anonymised (No personal data is collected within the PREMs and any identifying comments made will be redacted as part of the cleaning process.	-	Joint Controllers: HQIP and NHS England Processor: NPDA Sub processor: translation company (TBC)
Reporting of PREM data at unit/regional/national level.	Aggregated	-	Controller: Joint Controllers: HQIP and NHS England Processor: NPDA
Preparation and sharing of data for the HCL Implementation Strategy	Personal data (identifiable)	From the RCPCH to NHS England via secure electronic file transfer	Joint Controllers: HQIP and NHS England Processor: NPDA

Please see NPDA data flow map

Transferring personal data outside the UK

If personal data is being transferred outside of the UK, 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).

Personal data shall not be transferred to a country or territory outside the UK unless there is agreement with HQIP. Pseudonymised data may be shared outside the UK if that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data and in line with article V of GDPR.

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		
NHS number (England and Wales) or URN number (Jersey)	Y		In order to track patient through audit years and to enable linkage with NHS England datasets
Address	N		
Postcode	Y		Used to derive LSOA and deprivation information to track outcome inequalities.
Date of birth	Y		To calculate age and eligibility for inclusion in some age-based analyses.

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]*
Date of death	Y		To remove these patients from certain denominators.
Age	N		Derived from birth date.
Sex	Y		Used to identify risk factor, risk adjustment.
Marital Status	N		
Gender	Y		For risk adjustment, and monitoring of inequality in outcomes.
Living Habits	N		
Professional Training / Awards	N		
Income / Financial / Tax Situation	N		
Email Address	N		
Physical Description	N		
General Identifier e.g. Hospital No	Y		Used to ascribe outcomes
Home Phone Number	N		
Online Identifier e.g. IP Address/Event Logs	N		
Website Cookies	N		
Mobile Phone / Device No	N		
Device Mobile Phone / Device IMEI No	N		
Location Data (Travel / GPS / GSM Data)	N		
Device MAC Address (Wireless Network Interface)	N		
Sensitive Personal Data			
Physical / Mental Health or Condition	Y		Microvascular/ macrovascular disease indicators to monitor diabetes outcomes, indicators of coeliac and thyroid disease to monitor prevalence of comorbidities, and indication of comorbid psychological distress.
Sexual Life / Orientation	N		
Family / Lifestyle / Social Circumstance	Y		Smoking status as an additional risk factor for CVD.
Offences Committed / Alleged to have Committed	N		
Criminal Proceedings / Outcomes / Sentence	N		

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]*
Education / Professional Training	N		
Employment / Career History	N		
Financial Affairs	N		
Religion or Other Beliefs	N		
Trade Union membership	N		
Racial / Ethnic Origin	Y		Used to identify risk factors, risk adjustment, monitor inequality of care/outcomes.
Biometric Data (Fingerprints / Facial Recognition)	N		
Genetic Data	N		

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.

Patient characteristics of patients submitted to the audit are reflected back to the submitter in the form of a data quality and data completeness report after each submission so that their accuracy can be scrutinised. Clinical leads are also obliged to sign a form at the end of submission confirming that they have reviewed its 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 the public information leaflet and lay summary report, and clinic poster	Published on our website, distributed electronically to PDUs.	N/A
Individuals can access information held about them	Included in the privacy notice published online.	Individuals can request this directly from units. If we receive a request we will forward to the appropriate unit and we can provide details of the categories we collect. The trust is the data controller of the patient record and provide information to us from his. We cannot respond to requests as we do not have the necessary information to verify ID and guardianship or to deal with any safeguarding concerns. There is College guidance on how to deal specifically with clinical audit rights requests.	Right of Access: The personal data we hold about you is provided by your unit. We can let you know which categories of data we collect but you will need to contact your unit directly for a copy of your personal data as they are data controllers of your patient record.
Request erasure (right to be forgotten) in certain circumstances,	Included in the public information leaflet.	We do not have a legal obligation to provide this as the legal grounds for processing are that	Right to Erasure and Right to Object: The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the

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
making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes		processing of the data is necessary in the public interest in relation to ensuring a high quality standard of healthcare. However, we do give individuals the option to opt out, which they can request through their units. If we receive a request, we will remove identifiers from our database so the individual will no longer be identifiable	public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please let your unit know and they will remove you from the submission. Alternatively, you can contact the NPDA project team: NPDA@rcph.ac.uk and we will ensure that your personal identifiers are removed from our database.
Rectification of inaccurate information	Included in the public information leaflet.	We are not the data controllers of this data. As this information is provided by the trust who is the data controller, we do not have any means to verify the accuracy of the data, we rely on the data controller to inform us of any inaccuracies. The unit is therefore responsible for assuring the accuracy of the data before submission and is given the tools to be able to do this. We forward any requests to the unit.	Right to Rectification: Any requests to amend or update your personal data should be sent to your unit. If we receive any requests, we will forward these to the unit.
Restriction of some processing	Included in the public information leaflet.	The trusts will receive any right to rectification requests and therefore will inform us if there are any restrictions on processing. As we are not data controllers, we do not have the authority to make decisions about the restriction of processing if the data should already have been deleted. We do not have the relevant information to undertake	Right to Restriction: Any requests for restriction of processing should be sent to your Trust and they will inform us where applicable.

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
		guardianship/safeguarding or ID checks.	
Object to processing undertaken on some legal bases	Included in the public information leaflet.	We give individuals the option to opt out, which they can request through their units. If we receive a request, we will remove identifiers from our database so the individual will no longer be identifiable and included in the audit going forward.	Right to Erasure and Right to Object: The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. **In England, can I opt out of the NPDA via the National Data Opt Out?** In England, the National Data Opt-Out service allows patients aged 13 or over (or those with parental responsibility for patients under 13) to opt out of their information being used for purposes beyond their direct care. The Secretary of State for Health and Social Care, having considered the advice from the Health Research Authority Confidentiality Advisory Group, has decided that the National Data Opt-Out will not be applied to the NPDA. This is because applying the National Opt-Out could introduce bias to the data and make it difficult to monitor care safety and quality within healthcare providers, leading to poor quality of care and health services and jeopardising patient safety. It could also reduce the impact of the data on improving care locally and nationally. However, you can still opt out of your personal information being used for this audit. Please let your paediatric diabetes team know and they will remove you from the submission so that we don't receive your data. Alternatively, you can contact the NPDA team directly at npda@rcpch.ac.uk and we will ensure that your personal identifiers are removed from our database. The National Data Opt-Out will be applied to data shared for research purposes. **Can I opt out of the NPDA via any other means?** Yes. You can opt out by asking your paediatric diabetes team not to submit any

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
			data to the RCPCH for inclusion in the NPDA. You can also contact the NPDA team via npda@rcpch.ac.uk **Opting Out in Jersey**To exercise your right to opt-out of your data being used for national audit and research, you can email the Clinical Audit team at HSSClinicalAuditDepartment@health.gov.je. You can also request that the processing of your data for national audit purposes is restricted through the online form found at *your personal data rights.* Data of Jersey patients who have opted out will be excluded from data flows to England.
Complain to the Information Commissioner's Office;	Included in the public information leaflet.	Published on our website, distributed electronically to PDUSs. Individual can contact the ICO directly with a complaint via the email provided on our privacy notice to them. In Jersey, a data subject can contact the Jersey Office of the Information Commissioner.	You do also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at casework@ico.org.uk if you have concerns about the way your/ your child's personal data are being handled. If you live in Jersey you can complain to the Jersey Office of the Information Commissioner.
Withdraw consent at any time (if processing is based on consent)	Not applicable. In England and Wales, Section 251 approval is in place for the core audit and PREM data is submitted anonymously. Our legal basis for processing is necessary for performing a public task in the public interest in regards to ensuring a high	Not applicable.	Not applicable.

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
	quality of healthcare. In Jersey, processing is permitted under the Data Protection law 2018 under the legal basis of 'Public interest under the common law of duty of confidentiality'.		
Data portability (if relevant)	Not applicable.	Not applicable. Data is not collected directly from the data subject, part of a contract or based on consent.	Not applicable.
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs.	HQIP and NHS England are joint data controllers of data submitted to the NPDA by paediatric diabetes units in England. HQIP and Digital Health and Care Wales (DHCW) are joint data controllers for data submitted by PDUs in Wales. HQIP can also be contacted if you have any questions or concerns how your information is being used for the audit: data.protection@hqip.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 public information leaflet.	Published on our website, distributed electronically to PDUs.	The data collected are held on secure servers which meets all data protection legislative requirements and is hosted within the EU. Data will only ever be shared in a pseudonymised format (unless the requesting institution has its own legal basis for holding patient identifiable data) and only with the approval of HQIP. For HQIP to approve the request, the requestor must be able to demonstrate compliance with stringent data protection policies and arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants. Personal data shall not be transferred to a country or territory outside the EEA. Pseudonymised or summary data

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
			may be shared outside of the EEA as per the guidance referred to. Units in Jersey will share personal data with the NPDA audit which is based in the UK. The UK is deemed adequate by the EU, they are also deemed adequate by the Jersey Office of the Information Commissioner, so no further steps are required to ensure the transfer of your personal data between the UK and Jersey.
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 public information leaflet.	Published on our website, distributed electronically to PDUs. We are processing under schedule 6(e) and schedule 9(i) of GDPR	The NPDA has section 251 approval to collect patient identifiable data in England and Wales without explicit patient consent as its aims are considered to be in the public interest, as the audit will help improve standards of paediatric diabetes care. To find out more about section 251 approval, visit the Health Research Authority website. In Jersey, processing is permitted under the Data Protection (Jersey) law 2018 under the following legal bases: - Public interest under the common law of duty of confidentiality The NPDA shares data with NHS England as part of the Hybrid Closed Loop Implementation Strategy, as requested via a Data Provision Notice (DPN). This is permitted under the Health and Social Care Act 2012 Sections 259(1)(a) and 259(1)(b), which requires health and social care bodies in England who are identified in a DPN to provide the required data.
To know the purpose(s) for the processing of their information.	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs. The purpose has been identified on the Section 251 application.	The purpose of the audit is to monitor the number of different types of diabetes amongst children and young people on a national level and monitor and compare the quality of care received and outcomes achieved by children and young people receiving care from different paediatric diabetes units and regions.

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
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Not applicable	Not applicable- there is no statutory obligation for parents/patients to provide data to the NPDA.	Not applicable
The source of the data (where the data were not collected from the data subject)	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs. Data is supplied by hospital clinical units, and by patients and patients themselves in the case of the PREMS	To carry out this audit on behalf of HQIP, RCPCH is collecting patient data submitted by paediatric diabetes units (PDUs) relating to completion of recommended health checks performed for the children and young people receiving care from their service, as well as the results of these health checks. The full dataset collected can be viewed here.
Categories of data being processed	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs.	To carry out this audit on behalf of HQIP and NHS England (the joint data controllers), RCPCH (the data processor) is collecting patient data submitted by paediatric diabetes units (PDUs) relating to completion of recommended health checks performed for the children and young people receiving care from their service, as well as the results of these health checks. We are also collecting information directly from parents and patients on their experiences of care via our PREM surveys.
Recipients or categories of recipients	Included in the public information leaflet.	Pseudonymise data when sharing and only do so where approved by HQIP and have legal grounds to do so. When sharing this is done in a secure way. We only share where we have a legal basis to share.	Data may be shared with third parties for the purposes of service evaluation or quality improvement by external academic researchers. Data will only ever be shared in a pseudonymised format (unless the requesting institution has its own legal basis for holding patient identifiable data) and only with the approval of HQIP. For HQIP to approve the request, the requestor must be able to demonstrate compliance with stringent data protection policies and

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
			arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants. Personal data shall not be transferred to a country or territory outside the EEA. The NPDA also collaborates with the National Diabetes Audit managed by NHS England to produce audits of young adult care. This initiative involves the flow of patient identifiable data to trusted third party organisations (NHS England) under Directions under the Health and Social Care Act 2012 for linkage with their datasets. An annual audit report is published which is available publicly via our website and via data.gov.uk. All data is reported at the level of individual paediatric diabetes units so that no patient identifiable data will ever be published. Privacy information relating to this audit is available from NHS England. The NPDA has also shared data with NHS England to investigate the role of COVID-19 infection and Type 1 Diabetes in children, adolescents and young adults under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002. More information about the legislation is available here. Patient identifiable data collected from PDUs in England is shared with NHS England each quarter as part of the NHS England hybrid closed loop (HCL) 5-year implementation strategy. More information about the strategy is available here. This data will allow NHS England to reimburse integrated care boards for any HCLs purchased and provided to patients within their area. After patient identifiers have been removed from the data in this programme, data may be used for secondary research purposes. HQIP's Overarching Research Database Approval for the NCAPOP permits this re-use under S.251 of the NHS Act 2006 (Reference 24/CAG/0108). For more information on data sharing for uses outside of the NPDA, please see: NCAPOP Privacy Notice – HQIP

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
			International Transfer of Data between England and Jersey As Jersey is outside of the UK, this is considered an international transfer under UKGDPR, so additional checks need to be undertaken to ensure that any personal data has an equivalent level of data protection in both countries. The UK is deemed adequate by the Jersey Office of the Information Commissioner, and the UK have deemed Jersey as having an adequate level of protection, so no further steps are required to ensure the transfer of your personal data between the UK and Jersey.
The source of the personal data	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs.	To carry out this audit on behalf of HQIP and NHS England, the joint data controllers, RCPCH is collecting patient data submitted by paediatric diabetes units (PDUs) relating to completion of recommended health checks performed for the children and young people receiving care from their service, as well as the results of these health checks
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in the public information leaflet.	Published on our website, distributed electronically to PDUs. We will contact HQIP (data controllers of the audit data) at the end of the contract to find out what their written instructions are in relation to the data and follow their written instruction including deletion or return of any duplications and copies.	The NPDA team at the RCPCH acts as the data processor on behalf of HQIP and NHS England, who are the data controllers for the NPDA data. The RCPCH will hold the NPDA data for as long as it is contracted to deliver the NPDA. All data will be deleted or transferred back to HQIP within two weeks of the end of our contract.
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.	Not 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.

Each year, the NPDA includes information about approximately 35,000 children and young people with diabetes. There is likely to be a small increase on this number 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, undesired modification and disappearance of data	1	5	5	**Reduced**	The NPDA data capture system will have regular database backups which are carried out as per planned schedules agreed with the system developers. Patient identifiable information that is entered onto the NPDA data platform is stored on a secure server. Authorised hospital staff are able to view or access data entered by their own team. Users have individual log-ins and accounts can only be created by RCPCH staff with admin access to the	Adequate technical measures have been put in place to reduce the risk of a security incident by balancing the type of data being processed against the technical solutions available. If there is an incident, staff have received appropriate training and there is an appropriate procedure in place to contain the risk. By raising data protection awareness amongst unit staff,		Platform Provider NPDA Project Team

					platform or authorised users at each hospital. Users are required to use two factors of authentication to access the platform. When downloading patient identifiable data from the platform, users will receive a prompt reminding hospital staff that data extracts contain patient identifiable data, reminding the staff member that they are responsible for ensuring data are downloaded to a secure location. Only authorised employees will have access to the server. The data centre is ISO 27001 certified. We have checked that the data platform provider has appropriate information security policies and procedures in place for dealing with	this reduces the risk of an incident occurring.		

					information security and security breaches. All patient identifiable data retained within the system will be encrypted to AES 256-bit standards. Any downloads of data to the college servers will be done by authorised staff and saved to restricted folders, restricted to NPDA staff and system administrators. Individual log ins and passwords are used for administrators of the data collection platform. The management of the NPDA data on the RCPCH servers will conform to the Access Controls set out within the RCPCH Information Security and Data Protection and Confidentiality Policies. All staff handling identifiable data will undertake mandatory training on Data			

					Protection and Information security, and may be asked to complete advanced training.			
Duplicated copies of the same information stored in two different places	2	2	4	**Reduced**	The RCPCH NPDA Project Team have a data cleaning and validation procedure in place to manage this and will review the validation procedure on a regular basis. The main copies are kept on RCPCH servers and copies are also retained on the data platform for data completeness reports generated by the data entered can be viewed for previous years.	Raw data is held on the data collection platform server to enable production of data completion reports for the benefit of audit participants. The RCPCH holds a copy of this raw data, and creates a masterfile for analysis for subsequent cleaning (including removal of duplicate rows of data), validation, and analysis,.	June 2018	NPDA Project Team/ Platform Provider
Inadequate data sharing agreements in place when sharing information	2	3	6	**Eliminated**	HQIP data access request process is adhered to. The RCPCH NPDA project team will have informed subjects about possible data linkage via the project privacy notice.	To ensure that the DSA is fit for purpose and to obtain approval from HQIP as the Data Controller via its Data Access Request Group (DARG).	As and when necessary	NPDA Project Team/ RCPCH DPO/HQIP DARG

					Participation Agreement is in place between HQIP and Jersey. The NPDA shares data with NHS England as part of the Hybrid Closed Loop Implementation Strategy, as requested via a Data Provision Notice (DPN). This is permitted under the Health and Social Care Act 2012 Sections 259(1)(a) and 259(1)(b), which requires health and social care bodies in England who are identified in a DPN to provide the required data.			
Inappropriate security on the system holding the data, including data being stored outside the EU.	1	5	5	**Reduced**	It is necessary to collect and download identifiable information since we need to be able to link NPDA data to the NDA dataset using NHS number and date of birth. We also need to be able to track the same patients across audit years using the same pseudocodes applied to each unique NHS number in each year. This	Reduces risk of data breach.	Already in place	Data Platform Provider NPDA Project Team

					ensures we maximise the potential for the data to be used in research. Patient identifiable information that is entered onto the NPDA data platform is stored on the server. Only authorised employees will have access to this server. The servers are based in the UK. The server is ISO 27001 certified. All patient identifiable data retained within the system will be encrypted to AES 256-bit standards. Any downloads of data to the college servers will be done by authorised staff and saved to restricted folders, restricted to NPDA staff and system administrators.			

					Individual log ins and passwords are used for administrators of the data collection platform. Users are required to use two factors of authentication to access the platform. The management of the NPDA data on the RCPCH servers will conform to the Access Controls set out within the RCPCH Information Security and Data Protection and Confidentiality Policies. All staff handling identifiable data have had or will undertake mandatory training on Data Protection and Information security, and may be asked to complete advanced training. NPDA does not store data outside of the EU. However, we may send this internationally for research subject to approval from HQIP as per their data access request process.			

Data collection seen as intrusive by individuals due to the opt out rather than consent approach.	2	2	4	**Reduced**	NPDA has an exemption from applying the national opt out in England which is explained in the privacy notice. The privacy notice also provides information to patient/carers on how they can still specifically opt out of their data being used in the audit.	Communicates the purpose and legal basis for processing data.	June 2023	NPDA Project Team
System for opt out is not robust enough	2	3	6	**Reduced**	All clinical leads sign a form confirming that no data have been submitted to the audit from patients wishing to opt out. The NPDA fair processing materials and privacy notices comply with new GDPR requirements in relation to fair and lawful processing and have been reviewed and approved by the RCPCH Head of Information Governance. The submitters are provided	The process ensures that patients and parents have a clear and effective way of exercising their right to opt out of participation in the audit, or to restrict processing of their data.	June 2023	NPDA project team

					with a data quality/completion report after each submission to be able to do accuracy checks and check anyone who should be removed has been removed. All patient-facing materials will link to the NPDA privacy notice webpage. The notices clearly explain to patients and parents the process for notifying their paediatric service directly and/or the RCPCH of any objections to the collection and use of their personal data for the purpose of NPDA. Patients/parents will also be provided with details on the project privacy notice of their rights under data protection legislation, including how to opt out. If parents/patients want to opt out, they need to inform their diabetes team, and any opt out requests made directly to the NPDA team will be			

					verified with their diabetes team. We have received an exemption from applying the national data opt out, which is also explained in the privacy notice.			
Future changes to the way data is used or shared. This may include the merger of datasets which may result in a wider dataset than individuals would expect.	2	3	6	**Accepted**	Processes and guidance will be reviewed on a regular basis and with any change to the project methodology. If we are considering merging datasets, we will first talk to the DPO about the GDPR implications and whether we need to make any changes to the privacy notice, or reconsider our legal grounds for processing. We will also update the DPIA to consider risks etc before any changes are made. Any additional risks or changes will be signed off by the Head of Information Governance.	Ensures timely review of communication and processes if there is a change in the project including updates to the privacy notice if there is a change in purpose.	NA	NPDA Project Team/ RCPCH DPO
Knowing when the data should be deleted	2	2	4	**Accepted**	The retention period of identifiers is conditional on the CAG Section 251 approval.	Ensures regular review if there are any changes to IG permissions or project methodology. Not	NA	NPDA Project Team/ RCPCH DPO

					The data will be retained for the duration of the audit. The current audit contract with HQIP as the commission body and data controller is due to run until May 2027. At the end of the contract, we will contact HQIP and ask for their written instruction as to whether the data will be returned or deleted. This will include any copies of data we hold, including those on our servers or sharepoint. Any redundant SharePoint workspaces will be deleted through the internal IS process. We do not have a system for reducing the amount of identifiable data within the system where patients have become adults or have died as this would limit the utility of this data for longitudinal research. Each new csv uploaded to the data capture system throughout the year triggers deletion of	keeping data longer than necessary.		

					previous submissions from same year so that duplicate/inaccurate data not retained. Back ups are in place at RCPCH in line with college policy. We do not have a process for de-identifying patient records within the system where patients have died or where patients have become adults and no further information has been submitted for X number of years since the entire dataset collected is an extremely valuable for longitudinal research where patient outcomes can be tracked through their life by linkage to other datasets including the NDA via their NHS number.			
Being able to rectify or delete the data if requested.	2	2	4	**Accepted**	Patients/Parents can inform their clinical team if they don't want their data to be included and participating Health Boards and Trusts can edit and update their	By having a process in place, this will ensure that RCPCH are able to answer rights requests in line with legal	May 2018	NPDA Project Team/ RCPCH DPO/HQIP

					own local data on the data platform using their secure login and password protected access. Patients/parents are informed about their rights to rectification and deletion of their data on the privacy notice. Our privacy notice states: "Right to Erasure and Right to Object: The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please let your unit know and they will remove you from the submission. Alternatively, you can contact the NPDA project team: NPDA@rcph.ac.uk and we will ensure that your personal identifiers	requirements and on time.		

					are removed from our database".			
Being able to update data regularly	1	2	2	**Accepted**	Participating Health Boards and Trust can edit and update their own local data on the data platform using their secure login and password protected access. Prospective data entry is possible throughout the audit year. Data quality and validation checks are carried out on the data prior to analysis for the national report. Previous years' data are accessible within the data capture system to enable units entering data via questionnaire to add data to these patient's records in the new audit year without setting up a new profile for each patient. This feature was added at the request of services who were finding it laborious	Health Board or Trust NPDA Designated Leads monitor and control the data that is entered into the audit platform and ensure via data quality checking functions that they are up to date with audit timelines and submission deadlines.		NPDA Project Team/ RCPCH DPO

					to re-register patients every year. Copies of information are held by the RCPCH team, currently on our servers, as we save versions of our analysis file during the validation and analysis process so that potential errors can be tracked back. Previous iterations of the Masterfile are saved in an archive folder.			
Being able to restrict processing of the data if requested.	2	2	4	**Accepted**	As per our privacy statements, we can restrict processing by deleting identifiers associated with pseudocodes given to patients already entered into the audit, and clinical leads sign off their data submissions stating that no patients who have opted out have been submitted.	Ensure that audit staff know how to deal with rights requests.	May 2018	NPDA Project Team/ RCPCH DPO
Individuals not adequately informed about their rights and how their data will be used	3	2	6	**Eliminated**	Finalise and publish the privacy notice/patient information leaflet which will include all of the information outlined in Articles 6 (1) (e) and 9 (2) (i) of GDPR. The DPO and CYP team will review the	By providing individuals with information about how their data will be processed and targeting it towards the audience, this will	First draft in May 2018 Second draft publishe	NPDA project team/RCPCH DPO

					notice to ensure it meets GDPR requirements but is also age appropriate (aimed at children aged 13 and above). This will be provided before any data is collected. Privacy notices will be reviewed annually with the College's DPO, and will be updated as applicable. Patient facing materials will link to the privacy notice webpage.	ensure individuals are fully informed about their rights and how their data will be used and are clear about their choice to opt out.	d Feb 2019 Updated June 2023	
Inadequate safeguards in place when transferring data overseas for the purpose of national outcome research	3	3	9	**Reduced**	Consult the DPO before sending any personal data outside of the EEA. We will only send to countries where either they are on the EU Commission approved adequacy list or where we have the UK International Transfer Agreements in place. Data will be minimised, anonymised where possible and pseudonymised. Data that is shared will be sent via encrypted means only. Transfer will only take place where an international transfer assessment has taken	By ensuring that adequate safeguards are in place, the information can be securely and legally shared. By minimising the amount of personal data this will reduce the risk.	Not decided yet.	NPDA project team/RCPCH DPO

					place. We will also have an information sharing agreement in place with each organisation that we share the data with if it is pseudonymised or minimised. Jersey is considered adequate by the UK and the UK is considered adequate by Jersey so no further safeguards need to be put in place. The RCPCH Head of IG will review this annually as part of the HQIP annual checklist process, as well as regularly check for any changes in adequacy decisions.			
Sub-processors processing on behalf of RCPCH do not have appropriate safeguards in place to protect the privacy rights of individuals	3	2	6	**Reduced**	RCPCH will carry out due diligence checks on all sub-processors before agreeing to contract by asking to see relevant information security and data protection policies or consent mechanisms being use (if applicable). RCPCH will also ensure that any contract with sub-processors includes the article 28 requirements for contracts with	This will ensure that only appropriate trustworthy sub-processors will be employed and will have certain legal obligations in relation to data protection under contract	31 May 2018	NPDA project team/ RCPCH DPO

					processors. We will also ensure that as part of the contract with our sub-processers they are required to inform us if they use any sub-processors.			
Corporate risks & compliance risks section								

What are the potential risks to the individuals whose personal data you hold?	**Probability of this happening** 1 Rare 2 Unlikely 3 Possible 4 Highly Likely 5 Almost certain	**Impact** 1 -minor 2-Moderate 3-Serious 4-Significant 5-Catastrophic	**Overall risk score** (PROBABILITY x IMPACT) + IMPACT	**Will risk be accepted, reduced or eliminated?**	**Current Mitigations**	**Actions Required**	**Expected completion date**	**Responsible owner**
IG not considered at the start of a new processing activity/system or procurement process- there is no data protection 'design by default'	2	3	9	Accepted	All staff aware of the PIA process and it is undertaken where there is a legal requirement. IG staff consulted on any new systems that manage data. AUP Policy in place covering use of college systems and adhered to. Children's code working group in place and compliance overseen by DPC. Process in place to ensure regular review of records for deletion (automated or manual).	By building data protection into new activities and systems at the beginning of the process, this not only reduces the risk of having to implement costly solutions earlier on, but ensure that data protection compliance is in place at the beginning. By having centalised IG processes, such as the PIA process, international transfer assessment and the childrens code working group ensures centralised oversight so that data protection is	Ongoing review by Data Protection Committee	Data Protection Committee

					Where staff will be undertaking a personal data transfer outside of the UK/countries with an adequacy decision, the transfer assessment form is completed on Topdesk and assessed by IG. Safeguarding mechanisms are put in place (e.g. International Transfer Agreements). IG will do an annual review of the information asset register and review if there is a change in adequacy decision to identify affected processes Digital involved in the procurement of any new IT systems.	built into projects and new processes. The AUP also provides staff awareness, ensuring all staff are informed of their responsibility. They are required to sign that they have read and understood this as part of the induction process.		

Inadequate IG Resourcing in place to meet minimal Legal Requirements:	2	3	9	Reduced	Minimal staffing in place to cover compliance work. IG budgets proportionate to IG requirements Data Protection Officer Appointed. Specialist training and development provided to IG staff as required. IG staff given designated time and resources to keep up to date with legislative changes Strengthen support from contract management team. Increased use of legal and IG consultancy to meet requirements	Part of budget process ensure adequate resourcing reflected for 2024/2025 Review consistent level of outsourced legal/IG consultant support. Engage with RC Data Protection group. Ensure regular learning and developmen t time for DPO, evidenced in PDR.	June 2024 Ongoing Ongoing	Data Protection Committee
Third parties processing personal data without due diligence checks and legally required accountability mechanisms	3	3	12	accepted	Article 28 contractual clauses in place with all data processors. DSAs in place where there is a DC-to-DC relationship.	1. Regular contract reviews (annual if data is high risk?) - Ensure major changes to legislation, technology or best	Ongoing review by Data Protection Committee	Data Protection Committee

					Centralised procurement process that includes required IG checks/due diligence. A processor can have many sub-processors so there needs to be a level at which due diligence is proportionate and a level of trust/risk acceptance. Centralised procurement process that includes required IG checks/due diligence. Centralised procurement process that includes required IG checks/due diligence and data destruction certificates are transfered to the College.	practice trigger relevant review(s) with suppliers.		
IG training awareness and culture: There is a lack of staff awareness in relation to	2	3	9	Reduced	Mandatory Data Protection	To undertake audit to establish	Ongoing review by Data	Data Protection Committee

information governance and staff are not trained on their responsibilities.					Training for all staff. Regular awareness campaign run by IG e.g. hub articles, town hall briefings, specialised training. Running regular phishing simulations. Running regular clear out days. Current training offered unlikely to meet requirements consistently. Need to identify and assess need, roles. (roles outside UK/EU) Ensuring privacy notices are in place and easily accessible to data subjects Publishing and regularly reviewing IG Policies, Procedures and Guidance.	current position all staff training - 95% completion of Data Protection eLearning (within 12 months 30th June 2023 - 30th June 2024) Immediate consideration to develop literature to disemmante on mass identify what constitutes handling of data and how this should be managed in line with role Privacy notices in situ and reviewed and republished in line with	Protection Committee	

					Regular reporting to SMT, AFRC and DPC.	line with legislation changes. To continue to update on The Hub, Huddles etc. Privacy notices in situ and reviewed and republished in line with line with legislation changes. To continue to update on The Hub, Huddles etc. Reporting matrix /AOB to be identified with submission dates established so this work can be scheduled as required. Process to be established to identify any		

						information that may be at risk, then to establish who will undertake audit		

Regularly reviewing the DPIA

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

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

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

Appendix 1 Submitting your own version of DPIA

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

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

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

Appendix 2 Guidance for completing the table

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

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