Data Protection Impact Assessment for the National Clinical Audit of Anxiety and Depression (NCAAD)

Document control:

	Name and role	Contact details
Document Completed by	Mary Dang Programme Manager (NCAAD)	Mary.Dang@rcpsych.ac.uk
Data Protection Officer name	Richa Sharma Head of Membership Services and Faculties	Richa.Sharma@rcpsych.ac.uk
Document approved by (this should not be the same person that completes the form).		
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5702659	

Date Completed	Version	Summary of changes
31 January 2020	V2	• Consultation dates with stakeholders • Removal of prospective audit tool information
11 April 2018	V1.1	N/A

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		Pseudonymised health data
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		Project is looking at care received by people with mental health difficulties (including those who lack capacity to consent to care) and will include the elderly, young people aged between 16 and 18 years old, and others who may be unable to consent (e.g. those with learning disabilities, asylum seekers and other vulnerable groups)
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		At present pseudonymised data is aggregated and compared to ONS data.
5.	Does your project match data or combine datasets from different sources?	Yes		Data is collected via care providers (NHS Trusts or organisations providing NHS-funded care). Privacy notice is available on the RCPsych website.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes		Data is collected via care providers (NHS Trusts or organisations providing NHS-funded care). Privacy notice is available on the RCPsych website.
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		Unable to identify individuals at national audit team level.
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	Yes		This is a new project

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.

In retrospect as part of GDPR compliance preparation.

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

The NCAAD is a three-year improvement programme, which was established to improve the quality of NHS-funded care provided to service users with an anxiety and/or depressive disorder in England. The audit has three components; a core audit on the care and treatment service users receive during and after a period of inpatient care for an anxiety and/or depressive disorder, and two 'spotlight' audits on key topics of relevance, one on psychological therapies and the other is a qualitative analysis of service user experience accessing psychological therapy.

The audit aims to:

- To enable NHS Trusts and organisations under contract to the NHS to improve the delivery of care to service users receiving treatment for an anxiety and/or depressive disorder in secondary care services;
- To provide comparative data on the quality of care provided by NHS Trusts and organisations under contract to the NHS to service users with an anxiety and/or depressive disorder;
- To provide comparative data on service user outcomes following treatment;
- To facilitate the development of effective quality improvement initiatives and share examples of best practice, enabling NHS Trusts and organisations under contract to the NHS to make the best use of audit data.

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.

Stakeholder Group	**Date Consulted**	**Comments**
NCAAD Implementation Group (includes Clinical Advisors, project team members, service user representative)	Monthly beginning July 2017 – May 2020	Implementation group discuss and agree methodology for audit (including data collection processes, data items collected, and reporting), this includes discussion about privacy issues.
NCAAD Steering Group (includes representatives from other professional bodies such as RCN and BPS, service user/carer charities and organisations such as Mind and Anxiety UK, service users and carers, HQIP and clinicians)	Six monthly beginning July 2017 - May 2020	Group discuss and agree methodology for audit (including high level data collection processes (detail agreed in Implementation Group) and data items collected), this includes discussion about privacy issues.
NCAAD Service User and Carer	Six monthly beginning	Group discuss and agree methodology for

Reference Group (includes 5 service users and carers, and McPin Foundation)	September 2017 - May 2020	audit (including high level data collection processes (detail agreed in Implementation Group) and data items collected), this includes discussion about privacy issues. Consultation also takes place electronically on specific items/tools for example review and feedback on the service user questionnaire including privacy and confidentiality statements.
Data Protection Officer and GDPR Consultant	Ongoing ad hoc from April 2018 - May 2020	As part of GDPR preparation, a review is ongoing.
Funders (HQIP)	Six monthly in NCAAD Implementation Group meetings beginning in July 2017 Quarterly contract review meetings beginning in October 2017	HQIP are members of our steering group and are involved in the same methodological discussions outlined above. GDPR is a standing item on the contract review agenda at present and we are actively liaising with our Project Manager and Information Governance team regarding our processes and GDPR compliance.
Prospective IT Provider (Net Solving)	From March 2018 – May 2020	The audit is in the process of procuring an IT solution. Feedback and information has been sought from the preferred provider regarding their compliance, security and processes.

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.

The DPIA will be updated on the webpage w/c 17 February 2020. https://www.rcpsych.ac.uk/improving-care/ccqi/national-clinical-audits/national-clinical-audit-of-anxiety-and-depression/resources-for-core-audit

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.

	Communications Mailing List	Registered Trust/Organisation Audit Contacts	Audit of Practice Dataset (Pilot Core Audit)	Audit of Practice Dataset (Core Audit)
Data source	Individual request, service contact mapping exercise (online information)	Submission from Trust/organisation via registration form. Minor amendments via email occasionally.	Submission from Trust/organisation via online form.	Submission from Trust/organisation via online form. Minor amendments will be done during data cleaning via email
Output	Correspondence (emails, letters)	Correspondence (emails, letters)	Slide set for steering group	Reports (National and Local)
Data shared with	N/A	N/A	N/A	StatsConsultancy – external statistician will be sent anonymised sections of data for analysis
Contains identifiable personal information?	Yes	Yes	Yes – Pseudonymised (identification only possible by submitting Trust/organisation)	Yes – Pseudonymised (identification only possible by submitting Trust/organisation)
Contains sensitive information?	No	No	Yes (see details below in section Error! Reference source not found.)	Yes (see details below in section Error! Reference source not found.)
Electronic Storage	Yes On network drive (with restricted access) On Dot Mailer account (accessible only with username and password) Shared email account (with restricted access)	Yes On network drive (with restricted access) On Dot Mailer account (accessible only with username and password) Shared email account (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)	Yes On network drive (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)	Yes On network drive (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)
Paper/Hard copy storage	No	No	No	No
Comments				

	Service User Survey Responses (Spotlight 1)	Therapist Survey Responses (Spotlight 1)	Audit of Practice Dataset (Spotlight 1)	
Data source	Submission from service user in receipt of psychological therapy	Submission from staff member providing therapy	Submission from Trust/organisation via online form. Minor amendments will be done during data cleaning via email	
Output	Reports (National and Local)	Reports (National and Local)	Reports (National and Local)	
Data shared with	N/A	StatsConsultancy – external statistician will be sent anonymised sections of data for analysis	StatsConsultancy – external statistician will be sent anonymised sections of data for analysis	
Contains identifiable personal information?	No – Anonymous	No – Anonymous	Yes – Pseudonymised (identification only possible by submitting Trust/organisation)	
Contains sensitive information?	Yes (see details below in section **Error! Reference source not found.**)	Yes (see details below in section **Error! Reference source not found.**)	Yes (see details below in section **Error! Reference source not found.**)	
Electronic Storage	Yes On network drive (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)	Yes On network drive (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)	Yes On network drive (with restricted access) SNAP webhost collects submitted forms (accessible only with username and password)	
Paper/Hard copy storage	Yes Stored in team office cupboard which is locked when unattended	No	No	
Comments				

Datasets are downloaded and stored on the internal drives once reports have been published. Registration and communications contacts are stored for the life of the audit (unless subject requests erasure). On closure of project HQIP requirements will be followed. Data is stored for the life of the audit plus 5 years as per guidance on restricted access drives.

Requests for data from the audit will go through the HQIP Data Access Request Group (DARG) as per HQIP guidance.

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).

Snap Surveys software uses US data centres all of which comply with ISO 27001. Clear contract and assurance provided in relation with GDPR requirements from provider. Only personal data included is name and surname relating to a staff member only at the point of registration to enable management of the audit.

Privacy Risk Register

Please see table below.

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	No		
NHS number	No		
Address	No		
Postcode	No		The service user's responsible CCG is collected. This will be able to narrow down their location to a wider area. Responsible CCG information allows the audit to identify areas in which CCGs may be performing better/worse than average and allow local CCGs to use the audit findings to improve practice/commissioning in their locality.
Date of birth	No		
Date of death	No		
Age	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of

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]*
			including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Sex	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Marital Status	No		
Gender	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Living Habits	Yes		Information about smoking (status and # cigarettes smoked per day), alcohol intake (units per week) and drug/substance misuse collected to assess whether interventions recommended by NICE have been appropriately offered/provided. Housing status - include
Professional Training / Awards	Yes		Spotlight audit collect information about Trust staff's therapy qualifications and professional background to identify who is providing psychological therapy and what training they have received to competently deliver the therapy provided. Previous audits indicated that a significant proportion of therapy is by someone who is not trained in the modality provided.
Income / Financial / Tax Situation	No		
Email Address	No		
Physical Description	No		
General Identifier e.g. Hospital No	No		
Home Phone Number	No		
Online Identifier e.g. IP Address/Event Logs	No		
Website Cookies	Yes		Snap Survey software uses cookies indicate previous responses to some types of survey (for example use of usernames) and enhance the functionality of the tools. The cookies used on the Snap Survey tools do not collect personal information.
Mobile Phone / Device No	No		
Device Mobile Phone / Device IMEI No	No		
Location Data (Travel / GPS / GSM Data)	No		
Device MAC Address (Wireless Network Interface)	No		
Sensitive Personal Data			

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]*
Physical / Mental Health or Condition	Yes		Specific diagnoses are collected to assess whether treatment offered is concordant with NICE guidelines. Multiple conditions/diagnosis is associated with poorer outcomes.
Sexual Life / Orientation	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Family / Lifestyle / Social Circumstance	Yes		Question asked about difficulties with their family/social circumstances to determine whether possible contributing factors towards the service users' difficulties were identified by the service during their assessment. Research suggests that those without strong family support/social networks have poorer outcomes. Additionally, it is suggested that there is a link between social isolation and higher incidence of anxiety/depressive disorders.
Offences Committed / Alleged to have Committed	No		
Criminal Proceedings / Outcomes / Sentence	No		
Education / Professional Training	Yes		Collected alongside employment status.
Employment / Career History	Yes		Collected alongside education status.
Financial Affairs	Yes		Questions include information about whether concerns with finances (e.g. debt) contribute to the service users illness. JUSTIFY
Religion or Other Beliefs	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Trade Union membership	No		
Racial / Ethnic Origin	Yes		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Biometric Data (Fingerprints / Facial Recognition)	No		
Genetic Data	No		
Use of Mental health legislation	Yes		Used to identify sections of MH act used to admit service users.
Interventions			Medication and psychological therapies
Spare			

Data quality standards for personal data

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

The first round of the NCAAD core audit and psychological therapies spotlight are retrospective audits taken at a specific point in time. Information will therefore not be updated should the information change post data cleaning.

Post submission, a data cleaning process will be carried out. This will highlight discrepancies between expected and received data. In addition, a random sample of Trusts/organisations will be selected to be visited by the audit team who will review the submitted data and case notes of a randomly selected cohort of service users.

A number of duplicate entries are required as part of data submission to assess inter-rater reliability. The first five cases will be double audited from each Trust/organisation for this purpose.

Contact information will be kept update manually (by amendment, removal etc.) by the team, or the subscription process in our bulk mailout software, Dot Mailer.

Access to the data highlighted above in the data information flow section, is restricted to those within the audit team. Data is saved on secure, access restricted drives, software and in email accounts, which cannot be accessed by those outside the team and organisation. Data shared with external contractors (e.g. external statistician) is anonymised and sent via secure encrypted email. Our contracts with our external data processors stipulate storage, confidentiality and access requirements.

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 Privacy notice. Service user and staff questionnaires include description of how data is being used. Posters and postcards used to publicise the audit and use.	Privacy notice on website and will be sent to participating Trusts etc. Questionnaires given in hard copy or online with information. Audit packs include publicity materials.	
Individuals can access information held about them	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
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	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Rectification of inaccurate information	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Restriction of some processing	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Object to processing undertaken on some legal bases	N/A – cannot identify individuals at national audit team level.		

	Requests would be directed to Trusts.		
Complain to the Information Commissioner's Office;	Would facilitate this as much as possible but we cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Withdraw consent at any time (if processing is based on consent)	N/A		
Data portability (if relevant)	N/A		
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Included in privacy notice.	Privacy notice on website and will be sent to participating Trusts etc.	
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 privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	Privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
To know the purpose(s) for the processing of their information.	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
The source of the data (where the data were not collected from the data subject)	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
Categories of data being processed	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	

Recipients or categories of recipients	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
The source of the personal data	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in privacy notice	Privacy notice on website and will be sent to participating Trusts etc.	
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	N/A		

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.

We have an expected sample of 4,000 individual service user submissions for the NCAAD core audit (audit of practice tool) which is currently in process. All of those 4,000 cases are pseudonymised with only the submitting Trust/organisation having access to the required information to identify the individual.

The expected sample size for the NCAAD psychological therapies audit (audit of practice tool) is expected to be in the same region, however the feasibility study which is currently being completed will provide a more reliable indication of the number of eligible service users. As part of this, we will also be collecting anonymous data from service users and therapists. The psychological therapies aspect of NCAAD is based on the previous National Audit of Psychological therapies which received data from 14,587 service users and 4,661 therapists. We expect the sample to be considerably smaller in the region of 5,000 service users and 3,000 therapists.

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**
Access by a non-authorised external agency/individual	2	2	4	**A**	Data is pseudonymised and cannot be linked to an individual or Trust/organisation without additional information.			
Access by a non-authorised internal College staff member	3	2	6	**R**	Review those who have access to folders and ensure only those who require access have it. Add passwords to files which are highly sensitive	Reduced number of people who may access information.	01 May 2018	FBG
External data hosting (Snap, Dot Mailer) have data breach	2	2	4	**A**	External system providers have high level of security in place and are compliant with international data security standards		01 May 2018	FBG
Data sent to incorrect person	2	2	4	**R**	All emails to be checked and logged in shared account by staff member. Passwords to be added to sensitive files	Double checking reduces likelihood of error. Logging of emails allows us to trace everything sent and recall where appropriate. Password protecting sensitive documents restricts access should it be sent	ASAP	FBG

Corporate risks & compliance risks section								

Regularly reviewing the DPIA

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

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

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

Appendix 1 Submitting your own version of DPIA

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

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

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

Appendix 2 Guidance for completing the table

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

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

Appendix 3: NCAAD Data Flow Diagram