

Data Protection Impact Assessment for National Confidential Inquiry into Suicide, Homicide and Safety in Mental Health (NCISH)

Document control:

	Name and role	Contact details
Document Completed by	**Rebecca Lowe, IG Lead**	**0161 275 0700** **Rebecca.lowe@manchester.ac.uk**
Data Protection Officer name	**Rebecca Lowe**	**As above**
Document approved by (this should not be the same person that completes the form).	**Dr Pauline Turnbull, Project Director**	**0161 275 0737** **Pauline.turnbull@manchester.ac.uk**
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z6787610**	

Date Completed	Version	Summary of changes
30/04/2018	**1**	
10/02/2020	**2**	**Updated to reflect national data opt-out**
02/11/2022	**3**	**Updated to reflect national data opt-out exemption and update of database figures**
06/09/2023	**4**	**Updated to reflect updated database figures and minor changes to content inc legal basis for processing.**
02/04/2025	**5**	**Updated with amendment to our secure data shredding provider.**
02/09/2026	**6**	**Updated with new study name and data flow**

Contents

Screening questions 4
Data Protection Impact Assessment 6
Purpose and benefits of completing a DPIA 6
Supplementary guidance 7
DPIA methodology and project information 7
DPIA Consultation 7
Publishing your DPIA report 8
Data Information Flows 9
Transferring personal data outside the European Economic Area (EEA) 10
Privacy Risk Register 10
Justification for collecting personal data 10
Data quality standards for personal data 12
Individual's rights 13
Privacy Risks 26
Types of Privacy risks 26
Risks affecting individuals 26
Corporate and compliance risks 26
Managing Privacy and Related risks 27
Privacy Risks and Actions Table 28
Regularly reviewing the DPIA 34
Appendix 1 Submitting your own version of DPIA 35
Appendix 2 Guidance for completing the table 37

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		Section 251 approval obtained. Majority of subjects are deceased. Impractical and inappropriate to seek consent from homicide perpetrators.
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		Section 251 approval obtained. Majority of subjects are deceased. Impractical and inappropriate to seek consent from homicide perpetrators.

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?	Y		Mortality data from the Office for National Statistics (ONS) and Homicide Index data from the Home Office and other UK country equivalent sources are linked with individual health records.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Y		Section 251 approval obtained. Majority of subjects are deceased. Impractical and inappropriate to seek consent from or individually supply privacy notice to homicide perpetrators. Data obtained from Office for National Statistics, Home Office and other UK country equivalent sources are linked with health records supplied by health organisations.

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.

In retrospect

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

The overall aim of the National Confidential Inquiry into Suicide, Homicide and Safety in Mental Health (NCISH) is to reduce suicide and homicide rates and improve patient safety overall.

Data collection is through a national case series of mental health patient suicide and homicide. We receive data from the Office for National Statistics and the Home Office and equivalent sources in other UK countries. This individual-level data is then shared with health organisations to identify whether the person had contact with mental health services in the year prior to death/offence. The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services.
For people who died by suicide and for perpetrators who committed homicide, a detailed questionnaire is completed by the clinician who was responsible for their care. Information from the questionnaires is not stored with any identifying data.

NCISH also undertake projects which may involve collecting information from additional sources.

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.

DPIA completed in consultation with the DPO, management team, senior management team, procurement team, data processors, IT, researchers, analysists and statisticians (originally on 30 April 2018).

The DPIA reflects the ongoing information management procedures of NCISH, which are regularly reviewed in our Information Security and Management Policy. NCISU information management procedures have been successfully audited twice by The Home Office and the Health and Social Care Information Centre.

Publishing your DPIA report

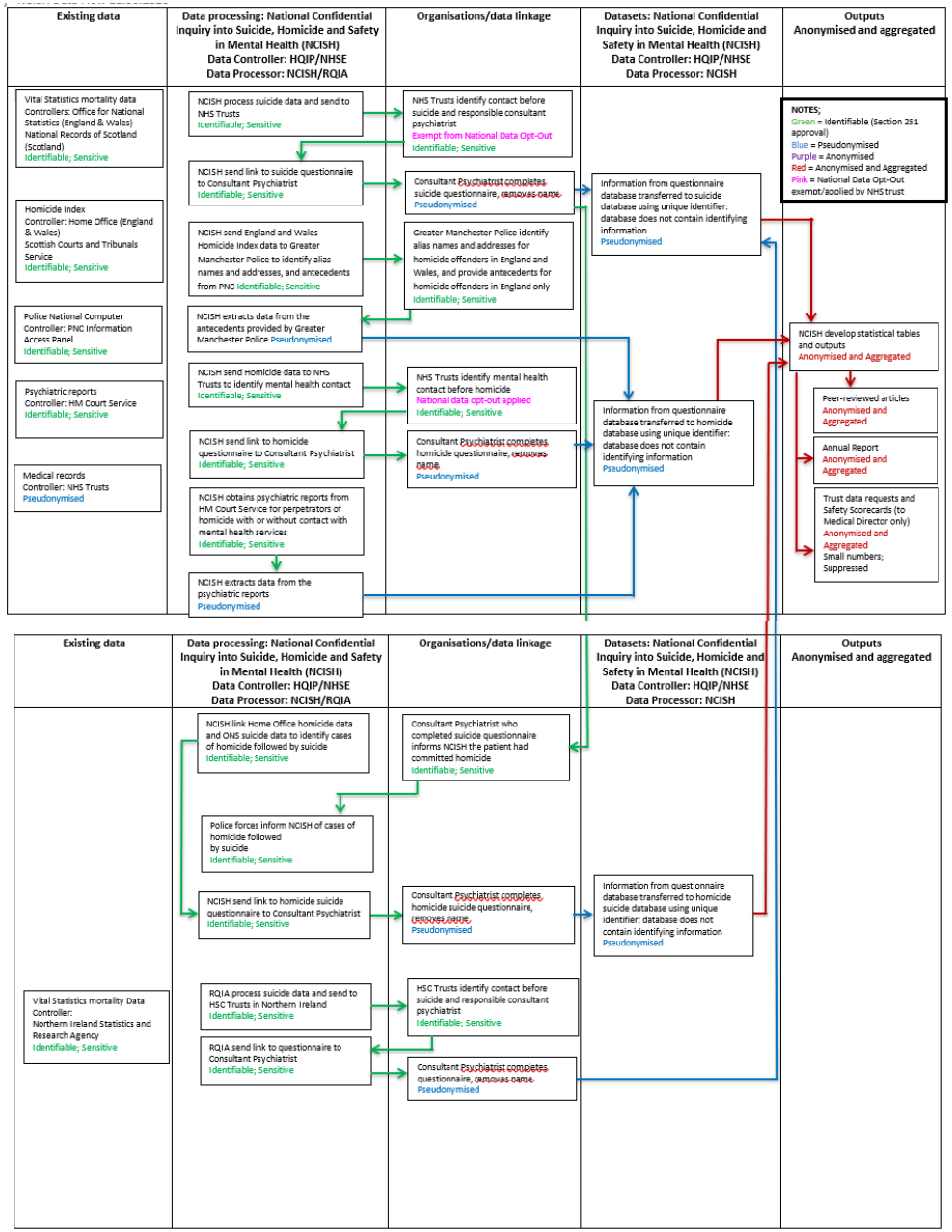
Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project 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 publish this DPIA on our website (www.manchester.ac.uk/ncish), alongside a privacy notice and a redacted version of our Information Security and Management Policy (ISMP) (redactions relate to business-sensitive information only).

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.



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).

N/A

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	Y		Needed in order to ascertain whether person had contact with mental health services.
NHS number	Y		Needed in order to ascertain whether person had contact with mental health services.
Address	Y		Needed in order to ascertain whether person had contact with mental health services, and under which services in terms of location
Postcode	Y		Needed in order to ascertain whether person had contact with mental health services, and under which services in terms of location.
Date of birth	Y		Needed in order to ascertain whether person had contact with mental health services. Also used to determine age.
Date of death	Y		Needed in order to ascertain whether person had contact with mental health services. Also used to determine age, year of death in relation to

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]*
			societal factors, and time of week/year in order to analyse timing.
Age	Y		Needed in order to analyse data and make age-specific recommendations.
Sex	Y		Needed in order to ascertain whether person had contact with mental health services. Needed in order to analyse data and make sex-specific recommendations
Marital Status	Y		Needed in order to analyse data - key variable for analysis
Gender	Y		Needed in order to analyse data - key variable for analysis
Living Habits	Y		Needed in order to analyse data - key variable for analysis
Professional Training / Awards	N		
Income / Financial / Tax Situation	N		
Email Address	N		
Physical Description	N		
General Identifier e.g. Hospital No	N		
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		Needed in order to analyse data - key variable for analysis
Sexual Life / Orientation	Y		Needed in order to analyse data - key variable for analysis
Family / Lifestyle / Social Circumstance	Y		Needed in order to analyse data - key variable for analysis
Offences Committed / Alleged to have Committed	Y		Needed in order to analyse data - key variable for analysis

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]*
Criminal Proceedings / Outcomes / Sentence	Y		Needed in order to analyse data - key variable for analysis/determining inclusion in study
Education / Professional Training	N		
Employment / Career History	Y		Needed in order to analyse data - key variable for analysis
Financial Affairs	N		
Religion or Other Beliefs	N		
Trade Union membership	N		
Racial / Ethnic Origin	Y		Needed in order to analyse data - key variable for analysis
Biometric Data (Fingerprints / Facial Recognition)	N		
Genetic Data	N		
Spare			
Spare			
Spare			

Data quality standards for personal data

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

NCISH is a retrospective study collecting data on patients who died by suicide or committed homicide. The information collected is about care received and circumstances prior to an index date (of death or offence). Therefore personal data is necessarily retrospective and would be inappropriate to keep up to date. The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by the National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH). This is due to overriding public interest in improving safety in clinical services.

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.	Majority of individuals are deceased. Section 251 approval obtained. The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services. Included in Privacy Notice	Privacy notice published on our website.	How will we use this information? We publish annual reports that include analysis of the most recent year of national data on patient suicides, as well as trends over time. In addition to annual reports, we publish project reports investigating specific patient sub-groups. We recommend changes to clinical practice and policy to reduce the risk of suicide and improve the safety of mental health patients. We only publish aggregate figures, and we follow ONS guidance about small numbers – we don't publish low counts, and we never share information about an individual. There are various retention periods for the differing data we receive, based on the specific requirements of the data providers and our

			overall Section 251 approval. Once a data destruction date is reached, the data are securely destroyed.
Individuals can access information held about them	Majority of individuals are deceased. Section 251 approval obtained. Included in Privacy Notice	Privacy notice published on our website	How do I get a copy of my personal information held by NCISH? If you believe that NCISH hold personal information about you, you have a right to ask for a copy of that information. This is commonly called a Subject Access Request (SAR). **Requests for medical (health) records** A request for information from health records has to be made with the organisation that holds your health records - the data controller. For hospital health records, contact the records manager or patient services manager at the relevant hospital trust**.** You can find a list of hospital trusts on the NHS Choices website. If you would like to receive a copy of other information we hold about you, your request should be made in writing (or email) to: • **Post:** NCISH, PO Box 86, Manchester, M20 2EF • **Email:** ncish@manchester.ac.uk Please include the words 'Subject Access Request' at the beginning of your letter or in the subject line of your email. When making your request, please include the following details: • Your name, address and postcode

			• The type of information you want to look at including any relevant dates We aim to send you a reply as soon as possible and by the latest within 30 calendar days. You may also be asked to provide proof of identity.
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	This does not apply as we are conducting a scientific research project	n/a	n/a
Rectification of inaccurate information	Majority of individuals are deceased. Section 251 approval obtained. Included in Privacy Notice	Privacy notice published on our website	Right to correct inaccurate personal information You have the right to request that any personal data that is inaccurate be rectified If you would like to request that personal data that we hold about you be corrected, your request should be made in writing (or email) to: • **Post:** NCISH, PO Box 86, Manchester, M20 2EF • **Email:** ncish@manchester.ac.uk Please include the words 'Request for Rectification' at the beginning of your letter or in the subject line of your email. When making your request, please include the following details: • Your name, address and postcode • Details of the inaccuracy We aim to send you a reply as soon as possible and by the latest within 30 calendar

			days. You may also be asked to provide proof of identity.
Restriction of some processing	Majority of individuals are deceased. Section 251 approval obtained. Included in Privacy Notice	Privacy notice published on our website	Request to restrict processing The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services. The right to restrict processing is not an absolute right and applies only in specific circumstances: • Where you contest the accuracy of your personal data and we need to verify the accuracy of the data; • The personal data were unlawfully processed (i.e. otherwise in breach of the DPA2018 & GDPR), and you request restriction rather than erasure of the data; • Where the personal data are no longer necessary in relation to the purpose for which it were originally collected/processed, but you need us to keep the data in relation to a legal claim; • When you object to the processing and we are considering whether our legitimate interest for continuing the processing would override this objection. If you would like to request a restriction of processing of your personal data, your request should be made in writing (or email) to: • **Post:** NCISH, PO Box 86, Manchester,

			M20 2EF • **Email:** ncish@manchester.ac.uk Please include the words 'Request to Restrict Processing' at the beginning of your letter or in the subject line of your email. When making your request, please include the following details: • Your name, address and postcode • The grounds for your request for erasure We aim to send you a reply as soon as possible and by the latest within 30 calendar days. You may also be asked to provide proof of identity.
Object to processing undertaken on some legal bases	Majority of individuals are deceased. Section 251 approval obtained. Included in Privacy Notice	Privacy notice published on our website	Right to object to processing The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services. You have the right to object to the processing of your personal data • Based on legitimate interests of the performance of a task in the public interest/exercise of official authority; • Direct marketing; • Processing for the purposes of scientific/historical research and statistics. You must have an objection on grounds relating to your particular situation. If you would like to raise an objection to the processing of your data, your objection

			should be made in writing (or email) to: • **Post:** NCISH, PO Box 86, Manchester, M20 2EF • **Email:** ncish@manchester.ac.uk Please include the words 'Object to Processing' at the beginning of your letter or in the subject line of your email. When making your request, please include the following details: • Your name, address and postcode • Details of the grounds for your objection We aim to send you a reply as soon as possible and by the latest within 30 calendar days. You may also be asked to provide proof of identity.
Complain to the Information Commissioner's Office;	Majority of individuals are deceased. Section 251 approval obtained. Included in Privacy Notice	Privacy notice published on our website	Report a concern to the Information Commissioner's Office You can report any concerns you have about our information rights practices to the Information Commissioner's Office (ICO): https://ico.org.uk/concerns/
Withdraw consent at any time (if processing is based on consent)	Data is collected without consent under Section 251. Data mostly relates to deceased individuals. Living individuals are those who committed homicide - data collected without consent from Home Office and health records.	n/a	n/a
Data portability (if relevant)	n/a	n/a	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 published on our website	Who is responsible for the data we collect? The National Confidential Inquiry into Suicide, Homicide and Safety in Mental Health (NCISH) is commissioned by the Healthcare Quality Improvement Partnership (HQIP). HQIP is led by a consortium of the Academy of Medical Royal Colleges, the Royal College of Nursing and National Voices. HQIP's aim is to promote quality improvement, and it hosts the contract to manage and develop the Clinical Outcome Review Programmes, one of which is the Mental Health Clinical Outcome Review Programme, funded by NHS England/Improvement, NHS Wales, the Health and Social Care division of the Scottish Government, the Northern Ireland Department of Health, and the State of Jersey. The programmes, which encompass confidential enquiries, are designed to help assess the quality of healthcare, and stimulate improvement in safety and effectiveness by systematically enabling clinicians, managers and policy makers to learn from adverse events and other relevant data. More details can be found here. -
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.	England	Privacy notice published on our website	NCISH and its data are based at the University of Manchester, which was established by Royal Charter.
To know the legal basis under	Processing is necessary	Privacy notice published	What rights do we have to

which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The University of Manchester was established by Royal Charter. Included in Privacy Notice	on our website	hold this information? Processing of the data that we hold is necessary in the public interest, for scientific and statistical research purposes in accordance with Article 89(1) of the General Data Protection Regulation. **Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.** Commissioning arrangements link to NHS England, Welsh, Scottish and Northern Irish Governments and other national bodies with statutory responsibilities to improve quality of health care services. **Article 9 (2)(I) (processing is necessary for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health
To know the purpose(s) for the processing of their information.	Included in Privacy Notice	Privacy Notice published on our website	How will we use this information? We publish annual reports that include analysis of the most recent year of national data on patient suicides, as well as trends over time. In addition to annual reports, we publish project reports investigating specific patient sub-groups. We recommend changes to clinical practice and policy to reduce the risk of suicide and improve the safety of mental health patients. We only publish aggregate figures, and we follow ONS guidance about small numbers – we don't publish low counts, and we never share information about an individual. The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services.

Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Personal data is not collected directly from data subjects, and is not part of a statutory obligation. Included in Privacy Notice	Privacy Notice published on our website	We do not collect information directly from data subjects, and this information is not part of a statutory obligation.
The source of the data (where the data were not collected from the data subject)	Office for National Statistics, National Records Scotland, NISRA, Homicide Index, GMP, Scottish Courts and Tribunals Service Included in Privacy Notice	Privacy Notice published on our website	What information do we collect? We collect information on people who have died by suicide, and some information on people who committed homicide. We receive identifying information about people who have been allocated a suicide or undetermined conclusion at coroner's inquest from the Office for National Statistics (ONS) (England and Wales), the National Register Office (NRS) (Scotland), and pseudonymised data from the Regulation and Quality Improvement Authority (RQIA), who manage identifying information from the Northern Ireland Statistics and Research Agency (NISRA). We also receive information identifying information about people who have committed homicide from the Home Office (England and Wales), the Scottish Courts and Tribunals Service, and Greater Manchester Police. The information we initially receive from these organisations includes people's names, addresses, dates of birth and death or offence, and cause of death or information related to the offence. We share this

			healthcare providers who let us know whether the person was in contact with mental health services in the year before death/offence. The National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services. For people who died by suicide, we collect detailed clinical information from the healthcare organisation they had contact with before death via an online questionnaire. No identifying information is collected on the questionnaire and any further correspondence with healthcare services uses a unique identifier that we generate in our office. The clinical information is held on a database which is not linked to the personal identifiable information.
Categories of data being processed	All categories of data collected can be seen in questionnaires published on our website	Questionnaires published on website	LINK
Recipients or categories of recipients	Only aggregate anonymised data is published - this is shared widely. Key audiences are identified in our Privacy Notice	Privacy Notice published on our website	Our key audiences are: • **People who receive care**: Patients & service users, their families & carers, the general public & press • **People who deliver care:** Mental health professionals, who provide us with our data and whose clinical practice is the main focus of our recommendations, medical/clinical

			directors, risk managers, trust chief executives & boards • **People who commission care:** CCGs, NHS England/Improvement, devolved governments including policy and practice leaders • **People who regulate care and provide national oversight:** CQC, NICE, Health Education England and equivalent bodies in all UK countries
The source of the personal data	Included in Privacy Notice	Privacy Notice published on our website	What information do we collect? We collect information on people who have died by suicide, and some information on people who committed homicide. We receive identifying information about people who have been allocated a suicide or undetermined conclusion at coroner's inquest from the Office for National Statistics (ONS) (England and Wales), the National Register Office (NRS) (Scotland), and pseudonymised data from the Regulation and Quality Improvement Authority (RQIA), who manage identifying information from the Northern Ireland Statistics and Research Agency (NISRA). We also receive information identifying information about people who have committed homicide from the Home Office (England

			and Wales), the Scottish Courts and Tribunals Service, and Greater Manchester Police. The information we initially receive from these organisations includes people's names, addresses, dates of birth and death or offence, and cause of death or information related to the offence. We share this information securely with healthcare providers who let us know whether the person was in contact with mental health services in the year before death/offence. National Data Opt-Out (where a person chooses not to have their health data shared for reasons beyond treatment and care) does not apply to suicide data collected by NCISH. This is due to overriding public interest in improving safety in clinical services. For people who died by suicide, we collect detailed clinical information from the healthcare organisation they had contact with before death via an online questionnaire. No identifying information is collected on the questionnaire and any further correspondence with healthcare services uses a unique identifier that we generate in our office. The clinical information is held on a database which is not linked to the personal identifiable information. We do not collect information directly from data subjects, and this information is not part of a statutory obligation.
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 published on our website	There are various retention periods for the differing data we receive, based on the specific requirements of the data providers and our

			overall Section 251 approval. Once a data destruction date is reached, the data are securely destroyed
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	n/a	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.

The current suicide database stands at 184060 suicides in the general population, including 46916 patients. There are around 7,000 suicides in the UK every year. The current homicide database stands at 18518 homicides in the general population, including 2630 patients. There are around 500 homicides in the UK every 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 You should include illegitimate access, undesired modification and disappearance of data?	**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**
Risk of security of data being compromised when data transfer occurs (from data providers and to NHS contacts) Sensitive, personal data on deceased individuals/homicide perpetrators is lost, stolen or destroyed. Could cause distress to any living data subjects/relatives **<u>Corporate risks & compliance risks</u>**. **Non-compliance with the DPA, principle 7 breached** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH	1		5	**R**	Data is accessed via a secure data exchange portal, as an encrypted email or via ZendTo . Data transferred using a password protected, encrypted pen drive and staff sign the pen drive in and out of the safe. Once data transferred, the data are deleted from the encrypted pen drive using FileShredder. Encrypted pen drive stored in fireproof safe in secure office, and used only for data transfer	By using encrypted pen drives this prevents unauthorised access to any data. The data portal can only be accessed via authorised NCISH staff via an encrypted laptop reducing the risk of hacking.. By deleting using FileShredder, the data cannot be recovered.	Completed – retrospective DPIA	Professor Louis Appleby

NCISH server could be hacked into and data stolen Sensitive, personal data on deceased individuals/homicide perpetrators is lost, stolen or destroyed. Could cause distress to any living data subjects/relatives **<u>Corporate risks & compliance risks</u>** **Non-compliance with the DPA, principle 7 breached** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH	1	5	5	**R**	Data stored on an isolated server and hosted on an isolated network which is not connected to any other network or the internet. All authorised PCs connected to this server have their hard drives fully encrypted. PCs are accessed via an encryption password, and individual access is managed according to need – not all members of staff have access to all drives.	This ensures that the network cannot be hacked into as it is not connected to the internet. Reducing access to the drives reduced the risk of unnecessary access to sensitive data	Completed – retrospective DPIA	Professor Louis Appleby
Security of data compromised by unauthorised personnel accessing data physically, i.e. within NCISH offices Sensitive, personal data on deceased individuals/homicide perpetrators is accessed by persons without authority **<u>Corporate risks & compliance risks</u>** **Non-compliance with DPA, breaching principles 1 and 7** Damage to reputation of NCISH and the University. ICO would be	1	5	5	**R**	Strict corridor management. Only authorised staff with security passes can enter the corridor and unauthorised personnel would be challenged upon entry. Data stored on an isolated server which is locked in an infrastructure cabinet in the NCISH office. All staff operate a clear desk policy. A password protected	Unauthorised personnel would not be allowed access to offices thus eliminating the risk of them being able to access data. The server being stored in a locked cabinet means that it cannot be accessed by anyone who should gain unauthorised access to	Completed – retrospective DPIA	Professor Louis Appleby

informed. Loss of confidence from clinicians to comply with NCISH					screensaver is activated after 10 minutes of inactivity on PCs.	the offices. The fact that nothing would be left on a staff members desk reduces the risk of an authorised personnel being able to access data in that way		
Risk of NCISH server being damaged or destroyed i.e. by fire Sensitive, personal data on deceased individuals/homicide perpetrators will be destroyed **<u>Corporate risks & compliance risks</u>** **Non-compliance with the DPA, principle 7 breached** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH	1	5	5	**R**	All data on server backed up overnight and a weekly backup tape is stored in a locked safe off site	This ensures that should a fire or flood occur we would still be able to restore the majority of lost data using back up tapes which are unlikely to have been affected by the fire/flood etc.	Completed – retrospective DPIA	Professor Louis Appleby
Risk that personal and sensitive data removed from the office by NCISH personnel via paper documents or on electronic devices Sensitive, personal	1	5	5	**A**	All NCISH staff are required to signed a Confidentiality Disclosure Agreement which states that no data can be removed	This remains an accepted risk although if any staff were to remove data that is not anonymised they would	Completed – retrospective DPIA	Professor Louis Appleby

data on deceased individuals/homicide perpetrators could be lost or damaged and potentially viewed by unauthorised personnel. **<u>Corporate risks & compliance risks</u>** **Non-compliance with the DPA, principle 7 breached** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH					from the NCISH office unless anonymised. Failure to comply would result in a disciplinary procedure. Regular checks carried out on staff laptops to check if any personal and sensitive data stored on them	be in breach of contract which would result in serious consequences for the staff member. Checking the laptops ensures that no one can store sensitive data on them		
Risk that personal data is retained for longer than is necessary Risk that a deceased individual's /homicide perpetrators data are held for longer than is needed and security methods applied to the data may lapse **<u>Corporate risks & compliance risks</u>** **Risk of breach of principle 5 of the DPA** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH	1	5	5	**R**	Data sharing agreements set up with data provider's state how long data can be retained for at the end of the project. These are collated in data destruction logs. There are also University guidelines regarding retention which must be adhered to.	Risk is reduced as guidelines are adhered to, to ensure that data is not retained any longer than is necessary, in line with data retention schedules.	Completed – retrospective DPIA	Professor Louis Appleby

Risk that personal and sensitive data which is sent out via the postal system could be opened by someone other than the intended recipient. Sensitive personal information on a deceased individual/homicide perpetrator could fall into the wrong hands, causing distress to living data subjects/relatives **<u>Corporate risks & compliance risks</u>** **Non-compliance with the DPA, principle 7 breached** Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH	2	5	10	**R**	No clinical data is sent out or received containing patient identifiable data. Correspondence which does include patient identifiable information is sent in an envelope marked CONFIDENTIAL and FOR ADDRESSEE ONLY. Patient identifiable information is sent via secure email where possible.	Risk is reduced as the majority of post does not contain any patient identifiable data. It cannot be eliminated completely but by marking the envelopes as detailed, reduces the risk of anyone opening the post who is not authorised to.	Completed – retrospective DPIA	Professor Louis Appleby
Risk that we request more data from data providers than we intend to use for purpose of the study Sensitive, personal information on deceased patients /homicide **<u>Corporate risks & compliance risks</u>** **Breach of principle 3 of the DPA**	1	5	5	**R**	NCISH only request data that is intended for the purpose of the work programme and data sharing agreements with the data providers make this clear. Some data suppliers send additional variables as these are automatically included in their	Risk reduced as we do not request data which are not used for the purpose of the work programme. Any additional data is not transferred to the NCISH secure server.	Completed – retrospective DPIA	Professor Louis Appleby

Damage to reputation of NCISH and the University. ICO would be informed. Loss of confidence from clinicians to comply with NCISH perpetrators is received despite it not being needed for the purpose of the study.					processes. Un-needed data is not transferred to the NCISH secure server.			

Regularly reviewing the DPIA

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

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

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

Appendix 1 Submitting your own version of DPIA

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

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

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

Appendix 2 Guidance for completing the table

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

	5	Catastrophic	Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved

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