

**Data Protection Impact Assessment for**

**National Audit of Care at the End of Life (NACEL)**

**V 6.0**

**Document control:**

|  |  |  |
| --- | --- | --- |
|  | **Name and role** | **Contact details** |
| Document Completed by | Debbie Hibbert,  Programme Manager, NHS Benchmarking Network team | debbie.hibbert@nhs.net |
| Data Protection Officer name  (Data Controller - HQIP) | Sacha Hewitt  Data Protection Officer | Sasha.hewitt@hqip.org.uk |
| Data Protection Officer name  (Data Processor - NHSBN) | Curtiss Green,  Data Protection Officer | curtiss@grgserv.co.uk |
| Document approved by | Claire Holditch, Director, NHS Benchmarking Network team | cholditch@nhs.net |
| Organisation’s ICO registration number  (Data Controller - HQIP) | Z1780946 |  |
| Organisation’s ICO registration number  (Data Processor - NHSBN) | This DPIA is completed by the NHS Benchmarking Network team, subcontractor to East London NHS Foundation Trust (ELFT) (host of the Network) on behalf of HQIP.  The Network (via ELFT) is contracted by HQIP to provide NACEL.  The Network team’s ICO number is Z1624069. |  |

|  |  |  |
| --- | --- | --- |
| **Date Completed** | **Version** | **Summary of changes** |
| 16th April 2018 | V1.0 | HQIP pilot template |
| 24th April 2018 | V2.0 | Revised HQIP template |
| 25th April 2018 | V3.0 | 30th April HQIP submission |
| 2nd May 2018 | V4.0 | Additional sections and comments from HQIP |
| 17th May 2018 | V5.0 | Approved by NACEL Steering Group (16/5/18) |
| 20th June 2018 | V6.0 | Update at request of HQIP on potential use of data for clinical audit, service evaluation & research purposes |

Contents

[Screening questions 4](#_Toc510712232)

[Data Protection Impact Assessment 5](#_Toc510712233)

[Purpose and benefits of completing a DPIA 5](#_Toc510712234)

[Supplementary guidance 5](#_Toc510712235)

[DPIA methodology and project information. 6](#_Toc510712236)

[DPIA Consultation 6](#_Toc510712237)

[Publishing your DPIA report 7](#_Toc510712238)

[Data Information Flows 8](#_Toc510712239)

[Transferring personal data outside the European Economic Area (EEA) 9](#_Toc510712240)

[Privacy Risk Register 10](#_Toc510712241)

[Justification for collecting personal data 10](#_Toc510712242)

[Data quality standards for personal data 12](#_Toc510712243)

[Individual’s rights 13](#_Toc510712244)

[Privacy Risks 15](#_Toc510712245)

[Types of Privacy risks 15](#_Toc510712246)

[Risks affecting individuals 15](#_Toc510712247)

[Corporate and compliance risks 15](#_Toc510712248)

[Managing Privacy and Related risks 16](#_Toc510712249)

[Privacy Risks and Actions Table 17](#_Toc510712250)

[Regularly reviewing the DPIA 19](#_Toc510712251)

[Appendix 1 Submitting your own version of DPIA 20](#_Toc510712252)

[Appendix 2 Guidance for completing the table 22](#_Toc510712253)

# 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? | No |  |  |
| 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. | No |  | Audit may include the elderly and their carers, who may also be elderly. However, no patient identifiable data is being collected. |
| 4. | Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals’ location or behaviour? | No |  |  |
| 5. | Does your project match data or combine datasets from different sources? | Yes |  | But only within the audit. Case note review data and carer survey data will be linked. |
| 6. | * Does your project collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’)? | No |  |  |
| 7. | * Does your project process data that might endanger the individual’s physical health or safety in the event of a security breach? | No |  |  |
| 8. | Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project? | Yes |  | Structure of the project is set out in the HQIP tender and response. |

# 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](https://ec.europa.eu/info/law/law-topic/data-protection_en) (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](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)
* ICO’s conducting [privacy impact assessments code of practice](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf)
* The [ICO’s Anonymisation](https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf): 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](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf) may help organisations to identify privacy risks associated with sharing personal data with other organisations.
* The [ICO’s codes of practice on privacy notices](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/), 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](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf) to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

## DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

During the planning stage of NACEL, which is a new project. The NACEL project is currently at the scoping stage of the three elements of the audit being delivered in the first year. The three elements are a case note review (all deaths during April 2018), linked to a carer reported measure, and an organisational level audit. This has been undertaken with the NACEL Steering Group and the NACEL Advisory Group. A Staff Reported Measure is being developed for Year 2 of NACEL.

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

The overall aim of NACEL is to improve the quality of care of people at the end of life in acute, mental health inpatient facilities and community hospitals. The audit is being undertaken in England and Wales. In terms of the three audit elements, the data collection methodologies are online data collection for the case note review and organisational level audit. The carer reported measure will be notification via post and online data collection via a unique URL following a linkage at the organisational level.

The objectives of NACEL are:

* To establish whether appropriate structures, policies and training are in place to support high quality care at the end of life.
* To assess compliance with national guidance on care at the end of life.
* To determine what is important to dying people and those important to them.
* To provide audit outputs which enable stakeholders to identify areas for service improvement.
* To provide a strategic overview of progress with the provision of high quality care at the end of life in England and Wales.

## 

## 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.

1. **Consultation since contract for NACEL was awarded**

Stakeholder engagement has been undertaken by the Network team to refine the scope and content of the audit and the consult on the impact on privacy risks. The engagement process includes:

* NACEL Advisory Group meeting 15th January 2018
* NACEL Steering Group meetings to date – 4th December 2018, 19th February 2018, 21st March 2018. The group will continue to meet monthly.

The data specification for the case note review will be signed off at the 16th April Steering Group meeting and the carer reported measure at the 16th May meeting. The privacy risks of the agreed content will be reviewed at these meetings.

Other consultation: -

* BMC Data Protection Officer
* The Patients Association is represented on the NACEL Steering Group and patient representatives are being consulted directly on the content of the carer reported measure.

## 

## 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 has been published on the NACEL web page.

## Data Information Flows

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential ‘function creep’, unforeseen or unintended uses of the data for example data sharing.

The data flow chart is embedded 

The chart illustrates how data is collected for the four elements of NACEL. The organisational level audit does not contain any personal information. Data is aggregated to a high degree e.g. number of deaths per annum in the hospital. The staff reported measure has not yet been scoped (Year 2).

The two elements of NACEL which include limited personal data (see next section) are the Case Note Review and the Carer Reported Measure.

**Legal basis for NACEL**

Under the new regulations, the legal basis for Trusts / UHBs to undertake clinical audit is direct care, dealt with under:

*Article 6(1)(e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority..’, using the Article 9 condition for direct care or administrative purpose 9(2)(h)@...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…’*

Trusts will be reminded that the audit should be identified as data sharing activity in line with data protection requirements and Trust / UHB fair processing notices should be reviewed to ensure compliance with new legislation.

The legal basis for NHSBN to process the data is under contract with HQIP, the Data Controller.

**Case Note Review data collection**

Data is anonymised and collected via an online portal, on a secure N3 connection to a server hosted by Midlands & Lancashire CSU within the NHS. Data is collected and input by the Trust staff undertaking the audit who may be clinicians or clinical audit managers. Access to the data collection portal is password protected. All users of the portal have unique log in details.

GDPR legislation applies to a ‘natural person’ which means living individuals. Therefore, GDPR is not relevant to the case note review element of the audit. However, a common law duty of confidence (which is English law defined by precedent over 200 years) applies to deceased individuals and generally applies to things in their health record that they may not have wanted their family to know about.

**Duty of confidentiality**

The only organisations that have access to directly identifiable data linked to deceased individuals are the data controllers (Trusts and Welsh UHBs) that are participating in the audit. The data transferred to NHS Benchmarking is anonymised, and data included in outputs will be anonymised and further aggregated.

As regards the duty of confidentiality, all data that is collected is obtained directly from deceased individuals clinical record and is factual with elements of that data already accessible via other means – as an example death certificate, coroner court or disclosure as part of the death notification process. There is no disclosure of confidential data to NHSBN since all data received by NHSBN is anonymised.

The risk of re-identification of the individual from the anonymised data is extremely low since:

* Data is held securely in the Network’s SQL database on a server hosted by the CSU.
* Only the Network Technical Team (3 individuals) and a CSU administrator have direct access to the SQL server and database.
* The Network Project Team (15 individuals) have indirect access to individual data items in the database via a password protected Administration Utility. To obtain a download of all the data items a request has to be made to the Technical team by the NACEL Project Team (4 individuals).
* De-identification of the data by an individual in the Network team, or sharing the data outside the team without the Director’s approval, is a breach of the Network’s Data Security Policy. (Very low risk event).
* De-identification of the data would, in any case, be difficult and would require a motive, knowledge of the data set and knowledge of other data sources such as ancestry.co.uk to obtain further data from death certificates. (Minimal risk).

The risk of losing data and it then being re-identified is therefore extremely low.

**Carer Reported Measure**

**Legal basis**

The above basis (direct care) would also function as the legal basis for the Trust / UHB to collect the data needed to contact the carer (name, address etc) for the NACEL Quality Survey. However, as this is less clear cut, it is suggested to participants that they confirm this with their Trust / UHB Information Governance (IG) team.

As regards the process for storing information about carers required for the audit, it will again be suggested that participants contact their local IG team to ensure your local Trust / UHB processes are followed.

The legal basis for the actual data collection from carers (taking the form of an online survey submitted to NHSBN) is explicit consent. Wording is included on the survey form to explain the use of the data to carers.

**Carer data collection**

Data is collected from carers/relatives via a web based survey form. A link to this form is provide to the carer in a letter sent by the Trust. The link is unique and can only be used once. The carer’s contact details are not shared with the Network. The data input by the carer is saved in the Network’s SQL database and data security applies as above.

**Deletion**

Data will only be shared under the direction of HQIP. Data will have the audit code removed before being returned to HQIP at the end of the contract and deleted from the Network database as required by the contract.

**Research**

The data from NACEL may be used for clinical audit, service evaluation or research purposes. All requests for the use of this data will be logged and managed via HQIP.

# 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).

# Privacy Risk Register

Not applicable.

# 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](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) (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 |  |  |
| Date of birth | NO |  |  |
| Date of death | YES |  | Required to enable analysis of whether care varies during the week. Also to calculate time from recognition of death to death, early recognition being a key principle of national guidance. |
| Age | Yes (CNR & CRM) |  | Required to provide an age profile of the audit sample. Assessment can then be made as to whether end of life care varies for different age groups. |
| Sex | NO |  |  |
| Marital Status | NO |  |  |
| Gender | Yes (CNR & CRM) |  | Required to provide a gender profile of the audit sample. Assessment can then be made as to whether end of life care varies for different gender groups. |
| Living Habits | NO |  |  |
| Professional Training / Awards | NO |  |  |
| 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 | Yes (CNR & CRM) |  | A unique audit code will be generated to link the Case Note Review and Carer Reported Measure. The Network will not be able to link this code to any patient identifiable information. The attempt to link the data is a requirement of the HQIP contract. |
| Website Cookies | NO |  |  |
| Mobile Phone / Device No | NO |  |  |
| Device Mobile Phone / Device IMEI No | NO |  |  |
| Location Data (Travel / GPS / GSM Data) | NO |  |  |
| Device MAC Address (Wireless Network Interface) | NO |  |  |
|  |  |  |  |
| **Sensitive Personal Data** |  |  |  |
| Physical / Mental Health or Condition | Yes (CNR & CRM) |  | Required to provide a profile of the cause of death for the audit sample. Assessment can then be made as to whether end of life care varies for different medical conditions. |
| Sexual Life / Orientation | NO |  |  |
| Family / Lifestyle / Social Circumstance | NO |  |  |
| Offences Committed / Alleged to have Committed | NO |  |  |
| Criminal Proceedings / Outcomes / Sentence | NO |  |  |
| Education / Professional Training | NO |  |  |
| Employment / Career History | NO |  |  |
| Financial Affairs | NO |  |  |
| Religion or Other Beliefs | Yes (CNR & CRM) |  | Required to provide a profile of the religious affiliations for the audit sample. Assessment can then be made as to whether end of life care varies for different religious groups. |
| Trade Union membership | NO |  |  |
| Racial / Ethnic Origin | Yes (CNR & CRM) |  | Required to provide a profile of the ethnicity of the audit sample. Assessment can then be made as to whether end of life care varies for different ethnic groups. |
| Biometric Data (Fingerprints / Facial Recognition) | NO |  |  |
| Genetic Data | NO |  |  |
| Admission date and time | Yes (CNR) |  | As data will be pseudonymised, the Network will not be able to link this data to any patient identifiable data. |
| Date and time of death | Yes (CNR) |  | As data will be pseudonymised, the Network will not be able to link this data to any patient identifiable data. |

## 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.**

N/A

No patient identifiable data will be held by the Network.

# 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 participating Trust Privacy notices | Trust responsibility to ensure their Privacy Notice is accessible |  |
| Individuals can access information held about them | N/A |  |  |
| 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 |  |  |
| Rectification of inaccurate information | N/A |  |  |
| Restriction of some processing | N/A |  |  |
| Object to processing undertaken on some legal bases | Included in participating Trust Privacy notices |  |  |
| Complain to the Information Commissioner’s Office; | Included in participating Trust Privacy notices |  |  |
| Withdraw consent at any time (if processing is based on consent) | N/A |  |  |
| Data [portability](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-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 participating Trust Privacy notices |  |  |
| 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 participating Trust Privacy notices |  |  |
| To know the [legal basis](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/) under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis? | Included in participating Trust Privacy notices |  |  |
| To know the purpose(s) for the processing of their information. | Included in participating Trust Privacy notices |  |  |
| Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data. | N/A |  |  |
| The source of the data (where the data were not collected from the data subject) | Included in participating Trust Privacy notices |  |  |
| Categories of data being processed | Included in participating Trust Privacy notices |  |  |
| Recipients or categories of recipients | N/A |  |  |
| The source of the personal data | N/A |  |  |
| To know the period for which their data will be stored (or the criteria used to determine that period) | N/A |  |  |
| The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable) |  |  |  |

## Privacy Risks

## Types of Privacy risks

* Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
* Compliance risks e.g. breach of the GDPR
* Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

## Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual’s privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

Around 10,000 in each year of the audit.

It should be noted that it is the intention of the audit design that the Network never receives any patient identifiable information.

**Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.**

When completing the table you need to consider if:

* Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established information might be used for longer than necessary.

## Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

* Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
* Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

* Non-compliance with the common law duty of confidentiality
* Non-compliance with the GDPR.
* Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
* Non-compliance with sector specific legislation or standards.
* Non-compliance with human rights legislation.

## Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

* Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
* Implementing appropriate technological security measures.
* Ensuring that staff are properly trained and are aware of potential privacy risks.
* Developing ways to safely anonymise the information when it is possible to do so.
* Producing guidance for staff on how to use new systems and how to share data if appropriate.
* Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
* Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
* Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation’s behalf.
* Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

## Privacy Risks and Actions Table

**Please see appendix 2 for additional guidance on completing this table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **What are the potential risks to the individuals whose personal data you hold?** | **Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely  (See guidance below for definition)) | **Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition) | **Overall risk score**  (likelihood x impact = score) | **Will risk be accepted, reduced or eliminated?** | **Mitigating action to reduce or eliminate each risk**  **OR**  **Where risk is accepted give justification.** | **Explain how this action eliminates or reduces the risk** | **Expected completion date** | **Responsible owner** |
| Illegitimate access, undesired modification and disappearance of data | 1 | 1 | 1 | Eliminated | No patient identifiable data will be held.  No patient identifiable data will be transferred.  Any loss of anonymised data would not result in harm to any individual, since they can’t be identified.  Data is protected by the BMC Network and Data Security Policy. This includes that all BMC staff are Data Protection trained.  BMC are in the process of completing the new Data Security and Protection toolkit | Ensures that staff are aware of data protection risks and work within an agreed policy framework |  | Director NHSBN |  |  |
| Accidental receipt of patient identifiable data (e.g. carer such as a carer writing a name in a text box on the Carer Reported Measure online form | 1 | 1 | 1 | Eliminated | Random samples of the data will be scanned for any personal data.  Any breaches will be identified at the validation and review stage and dealt with on a case by case basis. However, it should be noted that such a breach could only happen by the carer themselves disclosing the information and hence gave consent. |  |  | Programme Manager NHSBN |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **Corporate risks & compliance risks section** |  |  |  |  |  |  |  |  |
| Reputational risk to the NHSBN if any personal data is ever inappropriately accessed | 1 | 1 | 1 | Eliminated | No patient identifiable data will be held.  No patient identifiable data will be transferred. Any loss of anonymised data would not result in harm to any individual, since they can’t be identified.  Data is protected by the BMC Network and Data Security Policy. This includes that all BMC staff are Data Protection trained.  BMC are in the process of completing the new Data Security and Protection toolkit | Ensures that staff are aware of data protection risks and work within an agreed policy framework |  | Director NHSBN |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# 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](#_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](#_Individual’s_rights) |  |  |
| Are safeguards in place surrounding international transfer? See section on [sending information outside the EEA](#_Transferring_personal_data) |  |  |
| Was [consultation](#_DPIA_Consultation) of the document carried out and with whom? |  |  |
| [Organisations ICO registration](https://ico.org.uk/esdwebpages/search) number |  |  |
| Organisations ICO registration expiry date |  |  |
| Version number of the DPIA you are submitting |  |  |
| Date completed |  |  |
|  |  |  |

# Appendix 2 Guidance for completing the table

|  |  |
| --- | --- |
| **What are the potential risks to the individuals whose personal data you hold?** | See examples above |
| **Likelihood of this happening (H,M,L)** | |  |  |  | | --- | --- | --- | | **Likelihood score** | **Description** | **Example** | | 1 | Very unlikely | May only occur in exceptional circumstances | | 2 | Unlikely | Could occur at some time but unlikely | | 3 | Possible | May occur at some time | | 4 | Likely | Will probably occur / re-occur at some point | | 5 | Very likely | Almost certain to occur / re-occur | |
| **Impact (H,M,L)** | |  |  |  | | --- | --- | --- | | **Impact scores** | **Description** | **Example** | | 1 | Insignificant | No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality | | 2 | Minor | 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 | | 3 | Moderate | 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 | | 4 | Major | 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 | | 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? |