East of England Ambulance Service NHS Trust

# Data Protection Impact Assessment Policy

| | |
|---|---|
| Document Reference | POL055 |
| Document Status | Approved |
| Version: | V5.0 |

| DOCUMENT CHANGE HISTORY | | |
|---|---|---|
| **Initiated by** | **Date** | **Author (s)** |
| Head of IG | July 2012 | Corporate Records Manager |
| **Version** | **Date** | **Comments (i.e. viewed, or reviewed, amended approved by person or committee)** |
| V1.0 | 30th July 2012 | Approved at EMT |
| V2.0 | 23rd February 2015 | Review date extension agreed by IGG following approval by EMB |
| V3.0 | 17th December 2015 | Review date extension approved by ELB |
| V3.1 | 19th October 2016 | Recommended by IGG |
| V4.0 | 17th November 2016 | Approved by ELB |
| V4.1 | February 2019 | Reviewed by Information Governance Team |
| V4.1 | March 2019 | Approved by Information Governance Group |
| V5.0 | 20 March 2019 | Approved by Management Assurance Group |

| | |
|---|---|
| Document Reference | |
| Recommended at<br>Date | Information Governance Group<br>12 March 2019 |
| Approved at<br>Date | Management Assurance Group<br>20 March 2019 |
| Valid Until Date | 2 years from approval date |
| Equality Analysis | Completed |
| Linked procedural documents | Data Protection Act 2018<br><br>Privacy and Electronic Communications (EC Directive) Regulations<br><br>Data Protection Impact Assessments Guidance (ICO) |
| Dissemination requirements | To all managers and staff via bulletins and intranet |
| Part of Trust's publication scheme | Yes |

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats

## Contents



### Appendices

## 1. Introduction

Privacy and data protection is as important as any other categories of risk managed in organisations today. The East of England Ambulance Service NHS Trust (EEAST) has to ensure that it meets its obligations under the Data Protection Act 2018 and ensure that data protection by design and default is embedded across the Trust. To assist with this, the Information Commissioner's Office (ICO) has developed the Guide to Data Protection and specifically, Data Protection Impact Assessments (DPIAs) to enable organisations to determine where within their processes there are risks to information created, maintained and processed by an organisation.

## 2. Purpose

This document is to assist staff undertaking a Data Protection Impact Assessment (DPIA) and defines the process to be followed when completing these assessments.

The purpose of a DPIA is to ensure that privacy and data protection compliance are built into any systems or processes that hold or process information. By using the DPIA process to identify any privacy concerns or risks this can in turn assist an organisation in determining how best to manage them.

The main reasons for undertaking a DPIA are:

- Identifying and minimising data protection risks, specifically compliance but also broader risks to the rights and freedoms of individuals
- Avoiding unnecessary costs and fines
- Ensure inadequate solutions are identified and rectified or changed.
- Avoiding loss of trust and reputation
- Informing the organisation's communications strategy
- Meeting and exceeding legal requirements

Completing DPIAs effectively will also help the Trust meets its obligations under the Data Protection Act 2018 and forms a key part of the new focus on accountability and data protection by design.

Under the new Data Protection Act 2018, there is a new obligation to complete a DPIA before carrying out types of processing likely to result in high risk to individuals rights and freedoms. If the DPIA identifies a high risk, the Trust has a duty to consult with the Information Commissioner Office.

## 3. Duties

### 3.1 Director of Clinical Quality and Improvement

The Director of Clinical Quality and Improvement has a responsibility to the Board for ensuring that any risks to privacy are managed and that DPIAs are undertaken to support this.

### 3.2 Directors

Directors are responsible for ensuring a DPIA is completed for any projects/processes/systems within their area. This can be delegated to either the managers of the project or someone within the project team.

### 3.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for ensuring all information risks are correctly identified, managed and that appropriate assurance mechanisms exist. The SIRO will be kept informed of DPIAs through the Information Governance Group meetings.

### 3.4 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian will be kept informed of DPIAs relating to patient information through the Information Governance Group meetings.

### 3.5 Data Protection Officer (DPO)

Has the leadership function for IG, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle person-identifiable information. The Data Protection Officer will be responsible for approving all DPIAs completed within the Trust.

### 3.6 Project Managers

Project Managers must ensure that a member of the project team is assigned to undertake the DPIA and that this person is given every assistance to complete this task

### 3.7 Information Governance Team

The IG team will support the project managers in completing the DPIA and provide advice in relation to completing the DPIAs. The IG team will ensure the DPO is made aware of all DPIAs for final approval.

### 3.8 All Staff

All staff must be aware of any privacy risks and should assist with the DPIA to ensure these are identified and managed.

### 3.9 Consultation and Communication with Stakeholders

The Trust is committed to involving staff and key stakeholders in the development, review and monitoring of key procedural documents.

## 4. Definitions

### 4.1 Processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Essentially this means any time we view, share, edit or delete information we are processing the data.

### 4.2 Screening Questions

The screening questions are used to determine if a DPIA is required, see appendix A.

### 4.3 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is an in-depth internal assessment of privacy risks and liabilities. This analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them. See Appendix B for the Trust's DPIA Template, based on the ICO template DPIA. The procedure for completing a DPIA is in Appendix C.

### 4.4 Data Protection by design and default

Data protection should be integrated into all of the Trust's processing activities and business practices, from the design stage rights through the lifecycle. The Data Protection Act 2018 requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. The Trust should consider the data protection implications of everything we do before we do it.

It also means the Trust should only process data that is necessary to achieve the specific purpose and links to the fundamental principles of data minimisation and purpose limitation. This should be specified beforehand within the DPIA.

The Trust can achieve this by ensuring the following are considered as part of any new data sharing or system implementation within the DPIA:

- Minimising the processing of personal data
- Pseudonymising personal data
- Ensuring transparency in respect of processing personal data
- Enabling individuals to monitor the processing
- Creating and improving security features.

The seven foundational principles of privacy by design (Information and Privacy Commissioner of Ontario) are implemented across the Trust and the DPIA process is the key way of ensuring this happens.

## 5. Document Development

### 5.1 Prioritisation of Work
DPIAs are a requirement for both the Data Security and Protection Toolkit and the Trust's legal obligations under the Data Protection Act 2018.

### 5.2 Identification of Stakeholders
All staff who work on the development of systems/processes/projects that may involve data handling are considered to be stakeholders here.

### 5.3 Responsibility for Document's Development
Overall responsibility for these Procedures lies with the Director of Clinical Quality and Improvement, with delegated responsibility passed to the Information Governance Team.

## 6. Consultation

Consultation is an important aspect of the DPIA, however this does not have to be a formal process and can be limited to the stakeholders who have a key interest in the project or those who may have the biggest concerns about the project. This phase can include consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

## 7. Equality Analysis

An Equality Analysis has been completed for this policy (Appendix E).

## 8. Monitoring

See Monitoring Table – Appendix D.

## 9. References

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

## 10. Associated Documents

Data Protection Act 2018
General Data Protection Regulations (GDPR)
Privacy and Electronic Communications (EC Directive) Regulations

**Appendix A Screening questions**

**Project Name**

**Project Lead**

**Date screening completed**

The below screening questions are to determine if a full-scale DPIA is required. These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.
Will the project involve the collection of new information about individuals?

**Will the project compel individuals to provide information about themselves? Does the information comprise of personal data or special category data?**

**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**

**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**

**Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**

**Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**

**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.**

**Will the project require you to contact individuals in ways that they may find intrusive?**

**Appendix B** **Data Protection Impact Assessment Template**

# Sample DPIA template

# Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

## Project details

| | |
|---|---|
| Name of manager completing DPIA | |
| Title of project | |
| Date DPIA completed | |

## Step 1: Identify the need for a DPIA

| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| --- |
| |

## Step 2: Describe the processing

| **Describe the nature of the processing**: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
|---|
| |

| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
|---|
| |

| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
|---|
| |

| **Describe the purposes of the processing**: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
|---|
| |

## Step 3: Consultation process

| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
|---|
| |

## Step 4: Assess necessity and proportionality

| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
|---|
| |

## Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

## Step 6: Identify measures to reduce risk

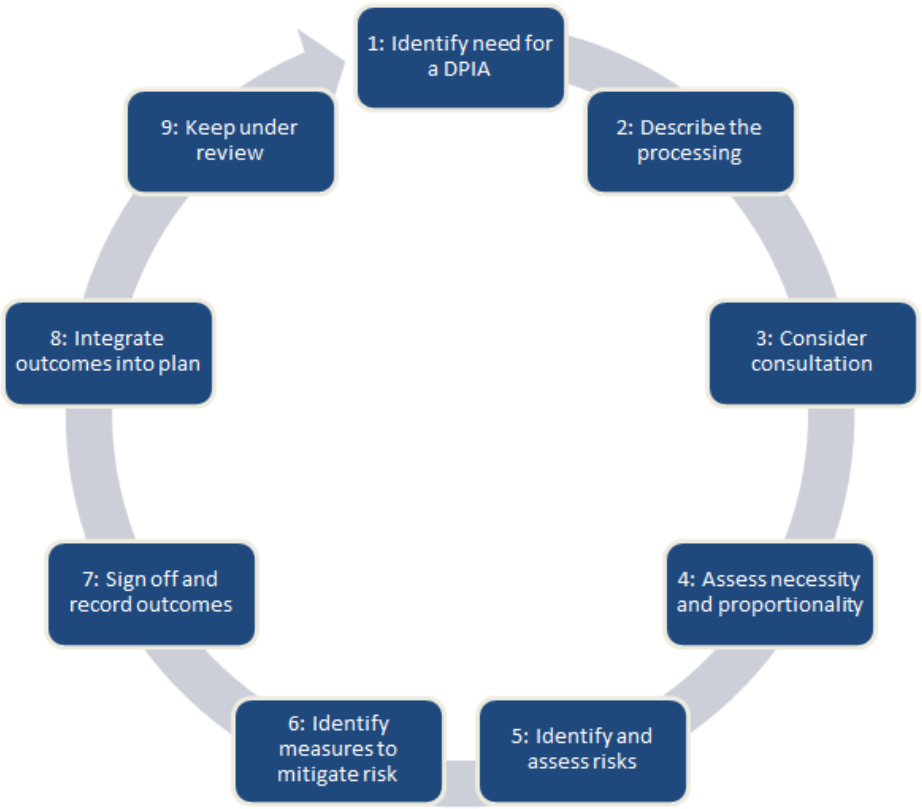
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| | | Eliminated<br>reduced<br>accepted | Low<br>medium<br>high | Yes/no |

## Step 7: Sign off and record outcomes

| Item | Name/position/date | Notes |
|---|---|---|
| Measures approved by: | | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | | The DPO should also review ongoing compliance with DPIA |

## Appendix C Procedure to complete a DPIA

The Trust has adopted the following process for conducting a DPIA (in line with ICO guidance):




### Procedure to complete a DPIA

### 1 Identifying the need for a DPIA

A DPIA must be completed before any processing of data is started that is 'likely to result in a high risk'. In particular under the new legislation, a DPIA must be completed if the Trust plans to:

Use systematic and extensive profiling with significant effects
Process special category or criminal offence data on a large scale
Or systematically monitor publicly accessible places on a large scale.

The ICO also requires a DPIA to be completed if the Trust plans to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

The need for a DPIA should be identified as part of an organisation's usual project management process or by using the screening questions in Appendix A of this document. Once completed the screening checklist should be sent to the IG team to review and should be minuted at the Information Governance Group.

## 2 Describing the information flows

Describe the information flows of the project and how the data will be processed. Explain what 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.

## 3 Consider consultation with stakeholders

It is always advisable to discuss the DPIA with a member of the IG team and the Data Protection Officer, if appropriate (e.g. if high risk). Relevant staff and patient groups should also be consulted with if the project will impact upon their individual rights.

## 4 Identifying the privacy and related risks, including an assessment of the necessity and proportionality.

You need to identify any privacy or legal risks to both individuals (for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy, limitation of individual rights) and to the organisation (for example)damage to reputation, or the financial costs of a data breach.

You should consider the necessity of the project and if there will be an impact upon individual rights, you should assess if this is proportionate to the aims of the project. You should also consider data minimisation and pseudonymisation.

## 5 Identifying and evaluating privacy solutions or ways to mitigate the risk.

Explain how you could address each risk. Some might be eliminated altogether whereas other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach and think about the available resources, and the need to deliver a project which is still effective.

## 6 Signing off and recording the DPIA outcomes

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Make sure that the risks have been signed-off at an appropriate level, this can be done as part of the wider project approval. All DPIAs should be approved by the Data Protection Officer and taken to the Information Governance Group.

The Trust's website informs the public that DPIAs will be shared upon request.

## 7 Integrating the DPIA outcomes back into the project plan

The DPIA findings and actions should be integrated with the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

Record what you can learn from the DPIA for future projects.

## Appendix D Monitoring Table

| What | Who | How | Frequency | Evidence | Reporting arrangements | Acting on recommendations | Change in practice and lessons to be shared |
|---|---|---|---|---|---|---|---|
| **Identification and completion of DPIAs** | **The summarised DPIA and checklists must be passed to the IG Team** | **The DPIA and checklists will all be checked by the IG Team and minuted at the Information Governance Group. DPIAs will also be approved by the Data Protection Officer.** | **As often as a DPIA is completed** | **The summarised DPIA and checklists** | **Reports on these will go to the Information Governance Group** | **Information Governance Group** | **The Information Governance Team will be responsible for implementing any accepted recommendations** |
| | | | | . | *The lead or committee is expected to read and interrogate any report to identify deficiencies in the system and act upon them* | *Required actions will be identified and completed in a specified timeframe.* | *Required changes to practice will be identified and actioned within a specific time frame. A lead member of the team will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders.* |

**Appendix E Equality Analysis**

| **Title: Data Protection Impact Assessment Procedures** |
|---|

| **What are the intended outcomes of this work?** *Include outline of objectives and function aims*<br><br>This document is to assist staff undertaking a Data Protection Impact Assessment (DPIA). The purpose of a DPIA is to ensure that privacy and data protection compliance are built into any systems or processes that hold information. |
|---|
| **Who will be affected?** *e.g. staff, patients, service users, general population etc*<br><br>All staff and third party contractors who are involved in the development of new projects or systems. |

| **Evidence** *The Government's commitment to transparency requires public bodies to be open about the information on which they base their decisions and the results.* [1] |
|---|
| **What evidence have you considered?** *List the main sources of data, research and other sources of evidence (including full references) reviewed to determine impact on each equality group (protected characteristic). This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations etc. If there are gaps in evidence, state what you will do to close them in the Action Plan on the last page of this template.* |
| **Disability**<br><br>The policy can be made available in different formats if required. |
| **Gender**<br><br>No evidence found to highlight any differences/ allowances required |
| **Race**<br><br>The policy can be made available in different formats if required. |
| **Age**<br><br>The policy can be made available in different formats if required. |

[1] EEAS Being Open Policy

| |
|---|
| **Gender reassignment (including transgender)**<br>No evidence found to highlight any differences/ allowances required |
| **Sexual orientation**<br>No evidence found to highlight any differences/ allowances required |
| **Religion or belief**<br>No evidence found to highlight any differences/ allowances required |
| **Pregnancy and maternity**<br>No evidence found to highlight any differences/ allowances required |
| **Carers**<br>No evidence found to highlight any differences/ allowances required |
| **Other identified groups**<br>No evidence found to highlight any differences/ allowances required |

| |
|---|
| **Engagement and involvement**<br>*Was this work subject to the requirements for public engagement/consultation?* |
| *How have you engaged stakeholders in gathering evidence or testing the evidence available?* |
| *How have you engaged stakeholders in testing the policy/strategy or programme proposals?* |
| *For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:* |

## Summary of Analysis

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

### Eliminate discrimination, harassment and victimisation

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

### Advance equality of opportunity

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

### Promote good relations between groups

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

### What is the overall impact?

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

### Addressing the impact on equalities

No actions required

## Action planning for improvement *Please give an outline of the key actions based on any gaps, challenges and opportunities you have identified. Actions to improve the policy/programmes need to be summarised (An action plan template is appended for specific action planning). Include here any general action to address specific equality issues and data gaps that need to be addressed through consultation or further research.*

Please give an outline of your next steps based on the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of EEAS strategic equality objectives.*

## For the record

**Name of person who carried out this assessment:**

Gail Butler (Corporate Records Manager)

**Date assessment completed:**

7th October 2016

**Name of responsible Director:**

Sandy Brown (Director of Nursing and Clinical Quality)

**Date assessment was signed:** 8th December 2016