London Ambulance Service NHS
NHS Trust

Data Protection Impact Assessment (DPIA) Policy and Procedure

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To outline the Trust's approach to the assessment of all new processes, services and systems at the project stage in order to ensure that they do not result in an adverse impact on information quality or a breach of information security, confidentiality, or Data Protection requirements.

.

Sponsor Department: Information Governance

Author/Reviewer: IG Manager. To be reviewed by May 2020.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
25/05/18	3.1	IG Manager	Document Profile & Control update
18/05/18	2.2	IG Manager	Major review and changes to comply with new DP legislation
17/10/17	2.1	IG Manager	Reviewed. No changes made.Major review required for 2018 to comply with GDPR.
07/09/16	1.5	IG Manager	Minor revisions following testing
28/09/15	1.4	IG Manager	Complete rewrite reflecting current ICO PIA Code of Practice
21/05/14	1.3	IG Manager	Amended draft
28/05/12	1.2	IG Manager	Doc Profile & Control update, new version of Appendix 6.1 and minor corrections
28/03/12	1.1	IG Manager	Reverted to one document as requested by ADG
13/03/12	0.4	IG Manager	Redrafted as separate policy and procedure
16/03/11	0.3	Head of Records	Refocused draft
16/07/2010	0.2	Head of Records	Revisions
29/06/2010	0.1	Head of Records	New document(As PIA P&P)

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
ELT	25/05/18	3.0
PMAG	14/09/16	2.0
IGG	30/09/15	1.4
ADG	27/03/12	1.0
Ratified by (If appropriate):		
SMG	16/05/12	1.0

Published on:	Date	By	Dept
The Pulse (v3.1)	25/05/18	Internal Comms team	Comms
The Pulse (v2.1)	01/02/18	Digital Media Officer	Comms
The Pulse (v2.0)	04/10/16	Governance Administrator	G&A
The Pulse	28/05/12	Governance Co-ordinator	G&C
LAS Website (v3.1)	25/05/18	Internal Comms team	Comms
LAS Website (v2.1)	01/02/18	Digital Media Officer	Comms
LAS Website (v2.0)	04/10/16	Governance Administrator	G&A
LAS Website	28/05/12	Governance Co-ordinator	G&C
Announced on:	**Date**	**By**	**Dept**
The RIB	05/06/18	IG Manager	IG
The RIB	11/10/16	IG Manager	G&A
The RIB	29/05/12	IG Manager	G&C

EqIA completed on	By
05/07/10	SRM; SM; BO.
Staffside reviewed on	**By**

Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
	Data Protection Act 2018	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

All organisations experience change in one form or another for various reasons including the need to develop and re-focus services to meet changing demands and requirements from both service users and funders. Technical requirements may also be a catalyst for change and it is vitally important to ensure that when new processes, services, systems, and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality, or data protection requirements. In particular the confidentiality, integrity, and accessibility of personal information must be maintained and such information must be processed safely and securely.

This policy covers the approach that must be taken by managers and staff in the London Ambulance Service NHS Trust to ensure that suitable Information Governance arrangements are in place when developing new products, services and processes and it includes integration into the Trust's approach to project management and the undertaking of Data Protection Impact Assessments where appropriate.

2. Scope

This policy applies to all departments and functions of the LAS and covers new or revised projects, processes or systems that are likely to involve a new use or a significant change to the way in which personal data is handled.

3. Objectives

3.1 To outline the Trust's approach to the assessment of all new processes, services and systems at the project stage in order to ensure that they do not result in an adverse impact on information quality or a breach of information security, confidentiality, or Data Protection requirements.

3.2 To provide the process for staff to carry out Data Protection Impact Assessments where required.

4. Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility for ensuring that Information Governance is managed responsibly within the Trust.

4.2 Director of Corporate Governance and Chief Information Officer (CIO)

The Director of Corporate Governance and the Chief Information Officer have strategic responsibility for Information Governance throughout the Trust. The CIO is the Senior Information Risk Owner (SIRO).

4.3 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and this policy supports the Caldicott function.

4.4 PMO and Business Improvement Director

The PMO and Business Improvement Director is responsible for ensuring that the Programme Management Office monitors the completion of DPIA's for all relevant projects.

4.5 Data Protection Officer

The Data Protection Officer is responsible for providing specialist data protection advice and for providing advice and developing specific guidance notes on data protection issues including completion of DPIAs.

4.6 Information Governance Manager

Responsible for the development of awareness and training packages and providing general advice to staff with regards to undertaking DPIAs and the implementation of this policy.

4.7 Information Security Team

Responsible for assessing information security aspects of new services, processes and systems and ensuring that mechanisms are in place for the protection of all personal identifiable data and other confidential material.

4.8 Information Governance Group

The Information Governance Group, jointly chaired by the Director of Corporate Governance and the Chief Information Officer, has strategic responsibility for monitoring the implementation of this policy, its effectiveness, and acting upon any risks or issues identified.

4.9 Directors, Senior Managers & IAOs

The Executive Leadership Team, heads of department and other managers who are Information Asset Owners (IAOs) are responsible for ensuring that the policy is implemented in their directorates and individual departments and a DPIA is undertaken for new processes and projects as required.

4.10 Managers

Project managers and other managers responsible for the introduction of new or revised service developments are required to ensure that their projects are assessed for their impact on information quality, information security, confidentiality, or Data Protection requirements using the project documentation and process as detailed in this document.

5. Definitions

5.1 Data Protection Impact Assessment – A process whereby a project’s potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and actions are undertaken to avoid or minimise privacy concerns.

5.2 Personal Confidential Data - data which directly identifies a living person or which, in combination with other data in the possession of a recipient, could be used to identify a living person.

5.3 Processing, in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as—

- collection, recording, organisation, structuring or storage,
- adaptation or alteration,
- retrieval, consultation or use,
- disclosure by transmission, dissemination or otherwise making
- available,
- alignment or combination, or
- restriction, erasure or destruction.

6. Assessments

6.1 All managers who are introducing or amending a service, process, or system must assess their project by following the methodology as detailed in the project management process and documentation as follows:

6.2 **Project Initiation Document (PID).** The Project Manager will carry out an initial screening in order to determine whether a Data Protection Impact Assessment is necessary and ensure that potential impacts on Information Quality at the design phase of any new process, and consideration of Information Security, including any risk to the integrity of information is documented by following the guidance in the PID. This includes involving the Information Security team to provide advice on appropriate security controls at this stage.

If the outcome of the initial screening indicates that a DPIA needs to be carried out it should be completed prior to the completion of the Project Initiation Document within the Initiation phase of the project. Where necessary any changes to the PID following the DPIA should be reflected in the document approved by the Project Board.

7. Background to Data Protection Impact Assessments (DPIAs)

7.1 Protecting the confidentiality of individuals has become a priority in recent years, and the development of new technologies has increased public concerns about the nature and extent of personal information collected by organisations and the impact of this on privacy. Privacy has been recognised as a significant risk factor for the London Ambulance Service NHS Trust (LAS) and the Information Commissioner's Office has developed a Data Protection Impact Assessments (DPIAs) Accountability and Governance document for organisations to use when developing and introducing projects and processes that may have an impact on how we use patient and staff information. NHS Digital (formerly HSCIC), via the Data Security and Protection Toolkit, have identified DPIAs as a key tool in addressing confidentiality and privacy concerns.

All new or significantly changed processes or projects that involve Personal Confidential Data that are planned to be introduced must comply with confidentiality, privacy and data protection requirements and the purpose of the DPIA is to highlight to the organisation any privacy risks associated with a project. They are structured assessments of the potential impact on privacy for new or significantly changed processes and should form part of the overall risk assessment of the process or project. They will help the LAS to:

- Anticipate and address the likely impacts.
- Identify privacy risks to individuals.
- Foresee problems.
- Negotiate solutions.
- Protect the reputation of the Trust.

Not every new or changed process will require a DPIA. However, a preliminary screening needs to be carried out in order to determine whether a DPIA is necessary. The Information Commissioner's Office recommends that DPIAs are used where a change of the law will be required, new and intrusive technology is being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way.

DPIAs are most effective when they are started at an early stage of the introduction of a process. Usually this is when the process is being designed and ideally before any systems have been procured. This ensures that privacy risks are identified and appreciated before they are implemented into the project design. It is suggested that the DPIA should be commenced as part of a project's initiation stage.

DPIAs should be conducted by someone that is introducing a new or significantly changed process that involves Person Identifiable Data. Usually a member of the Project Team such as the Project Manager, who is familiar with the project should be assigned the responsibility for undertaking the DPIA. FAQs are provided in Appendix 3.

The outcomes of the DPIA should be:

- The identification of the project's privacy impacts;
- Appreciation of those impacts from the perspectives of all stakeholders;
- An understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- Identification and assessment of less privacy-invasive alternatives;
- Identification of ways in which negative impacts on privacy can be avoided;
- Identification of ways to lessen negative impacts on privacy;
- Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- Documentation and publication of the outcomes.

8. Stages of a DPIA

The following are the main stages of a DPIA:

8.1 DPIA screening

In order to decide whether a DPIA is required a member of the project team, agreed by the project board, who is familiar with the project or initiative should use the Screening Questions at Appendix 1 to examine the project at an early stage, identify stakeholders, make an initial assessment of privacy risk and decide whether a DPIA is necessary. The DPO or Information Governance Manager must be advised so that the DPIA process can be registered and advice and training provided as appropriate. If the completion of the screening questions indicates that no DPIA is required the person responsible for undertaking the DPIA Initial Assessment should sign the document and send it to the DPO or Information Governance Manager.

8.2 The need for a DPIA is identified

If a DPIA is necessary Appendix 2 provides a template which should be used to record the results of each of the following steps:

8.3 Step one: The need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA.

8.4 **Step two: Describe the processing**
Describe the nature of the processing, the scope of the processing, the context of the processing and the purposes of the processing.

8.5 **Step three: Consultation process**
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?

8.6 **Step four: 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?

8.7 **Step five: Identify and assess risks**
Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

8.8 **Step six: 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.

8.9 **Step seven: Sign off and record the DPIA outcomes**

<table>
<tr><th colspan="5">IMPLEMENTATION PLAN</th></tr>
<tr><td colspan="2"><b>Intended Audience</b></td><td colspan="3">For all LAS staff who are responsible for the development of new or revised services, processes, projects and systems which contain or handle person identifiable information.</td></tr>
<tr><td colspan="2"><b>Dissemination</b></td><td colspan="3">Available to all staff on the Pulse</td></tr>
<tr><td colspan="2"><b>Communications</b></td><td colspan="3">Policy to be announced in the RIB and a link provided to the document</td></tr>
<tr><td colspan="2"><b>Training</b></td><td colspan="3">Training will be provided for all staff required to undertake DPIAs as part of the Information Governance training programme and advice will be available from the Information Governance Manager.</td></tr>
<tr><td colspan="5"><b>Monitoring:</b></td></tr>
<tr><td><b>Aspect to be monitored</b></td><td><b>Frequency of monitoring AND Tool used</b></td><td><b>Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported</b></td><td><b>Committee/ group responsible for monitoring outcomes/ recommendations</b></td><td><b>How learning will take place</b></td></tr>
<tr><td>Number of DPIAs completed</td><td>Quarterly reports</td><td>Information Governance Manager to
Information Governance Group</td><td>Risk Compliance and Assurance Group</td><td>Increase profile of DPIAs to managers as required</td></tr>
</table>

Appendix 1

Screening Questions – is a DPIA required?

To determine if a full DPIA is required the following questions must be answered.
If any of the answers to the following questions is "YES" then a full privacy impact assessment must be carried out.

Q	Category	Screening Question	Yes/No
1.1	Technology	Does the project / change introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy? E.g. Biometrics, tagging (rfid)	
1.2	Technology	Does the project / change introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business whether within a single function or across the whole business? E.G. data mining, shared hosting	
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, or will use intrusive identification or identity management processes?	
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	
1.5	Identity	Will the project / change compel individuals to provide information about themselves?	
1.6	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations? E.g. Integrated care records, Contracted private health care providers, Outsourcers in general, GPs, business partners	
1.7	Data	Does the project involve new process, policy or significantly change the way in which personal and/or business sensitive data is handled?	
1.8	Data	Does the project involve new or significantly	

		changed handling of a considerable amount of personal and/or business sensitive data about each individual in a database?	
1.9	Data	Does the project involve new or significantly change handling of personal data about a large number of individuals?	
1.10	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal and/or business sensitive data from multiple sources?	
1.11	Data	Will the personal data be processed out of the UK and / or EEA? Please give details	
1.12	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections? e.g. “251” exception	
1.13	Exemptions and Exceptions	Does the project’s justification include significant contributions to public security and measures?	
1.14	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	

If the answer is ‘No’ to all of the above questions the person responsible for undertaking the DPIA Initial Assessment should sign below and forward to the DPO or Information Governance Manager.

Signed……………………………....... **Date……………………………**

Name…………………………………….

Position…………………………………..

Appendix 2

Data Protection Impact Assessment template

This template should be used to record the DPIA process and results. Start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA. The completed assessment should be forwarded to the DPO or Information Governance Manager.

Step one: Identify the need for a DPIA

Explain broadly what the 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 two: 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 another 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:
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 three: 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 four: 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 five: Identify and assess risks

Describe the 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 six: 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, reduced or accepted	Low, medium or high	Yes/No

Step seven: Sign off and record the DPIA outcomes

Item	Name/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 be kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 3

FAQs

1. Who should carry out a Data Protection Impact Assessment?

Data Protection Impact Assessments (DPIAs) should be completed by key project personnel. This could be the project proposer (the person(s) who develops the project brief), project manager, or any other key project team member. It is likely that multiple staff from the project will need to be involved with carrying out the DPIA. It is essential that the person(s) undertaking the DPIA has clear knowledge of the project, the systems involved and the level of information required.

Therefore this document is for use by anyone who proposes or develops new systems/upgrades existing systems within the Trust. Assistance with following this process can be provided by the DPO.

2. What type of projects or systems require a Data Protection Impact Assessment?

The Information Commissioners Office envisages that DPIA's are required *only* where a project is:

of such a wide scope, or will use personal information of such a nature, that there would be genuine risks to the privacy of the individual.

3. At what stage of a project do I complete a Data Protection Impact Assessment?

The nature of the DPIA process means that it is best to complete it at a stage when it can genuinely affect the development of a project.

Carrying out a DPIA on a project that is up and running runs the risk of raising unrealistic expectations among stakeholders during consultation.

For this reason, unless there is a genuine opportunity to alter the design and implementation of a project, the ICO recommends that projects which are already up and running are not submitted to a DPIA process.

DPIAs are best conducted at the initial stage of an initiative to ensure that privacy concerns are identified. This ensures that they can be addressed and safeguards built in rather than bolted on as an expensive afterthought.
Recommendations include:-

- start early to ensure that project risks are identified and appreciated before the problems become embedded in the design.

- if possible, commence a DPIA as part of the PID (or its equivalent).

4. What are the benefits of completing Data Protection Impact Assessments?

The objective of the DPIA is to avoid the following **risks**:

loss of public credibility as a result of perceived harm to privacy or a failure to meet expectations with regard to the protection of personal information; patients, customers and staff value privacy.
A DPIA is a means of ensuring that systems are not deployed with privacy flaws which will attract the attention of the media, public interest advocacy groups or other stakeholders, or give rise to concerns among the public or staff. A DPIA will help to maintain or enhance an organisation's reputation.

retrospective imposition of regulatory conditions as a response to public concerns, with the inevitable cost that entails.

low adoption rates (or poor participation in the implemented scheme) due to a perception of the scheme as a whole, or particular features of its design, as being inappropriate.

the need for system re-design or feature retrofit, late in the development stage, and at considerable expense; in addition to avoiding the expense of resolving privacy problems at a later stage, performing a DPIA early in a project can help clarify a project's objectives, the organisation's requirements and the justifications for particular design features.

A further benefit of building privacy-sensitivity into the design from the outset is that it provides a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer life for the application.

collapse of the project, or even of the completed system, as a result of adverse publicity and/or withdrawal of support by the organisation or one or more key participating organisations. The kinds of projects that give rise to privacy concerns generally involve a considerable amount of effort and investment and those responsible for leading such projects need to ensure that risks are identified, assessed and managed.

That responsibility extends to checking whether privacy issues exist and, if so, assessing, developing and implementing a plan for managing these. As well as addressing project risk a DPIA is therefore part of good governance and good business practice.

compliance failure, through breach of the letter or the spirit of privacy law (with attendant legal consequences). Data Protection legislation already stipulates six

Data Protection Principles, but these only address certain aspects of privacy and DPIA's can also be taken into account.

5. How do I set up a Data Protection Impact Assessment?

In major initiatives, the most beneficial and cost-effective approach may be to conceive the DPIA as:

- a cyclical process
- □linked to the project's own life-cycle
- □re-visited in each new project phase

Conducting a DPIA usually requires diversity of expertise and interests and DPIAs are not usually conducted by one person but may require input from others so together they have expertise in a number of areas:-

- knowledge of the overall project
- knowledge of the relevant stakeholders and customer segments
- knowledge about privacy and the law
- expertise in project management
- expertise in records management, information management and data
- management
- expertise in relevant technologies
- expertise in information security processes and technologies
- knowledge of appropriate representatives of and advocates for the stakeholder groups and consultation techniques

6. How do I conduct a Data Protection Impact Assessment?

DPIAs are more than simply a data protection compliance check and are aimed at looking at all aspects affecting privacy.

The recommended approach involves a number of elements detailed in S8 of the policy.

The important thing about DPIAs is the process of undertaking the assessment where the Trust considers the impact on privacy and whether there are more privacy friendly alternatives.

7. What are the end results of an effective DPIA?

Ideally the end results of an effective DPIA are:

- the identification of the project’s privacy impacts;
- appreciation of those impacts from the perspectives of all stakeholders;
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it;
- identification and assessment of less privacy-invasive alternatives;
- identification of ways in which negative impacts on privacy can be avoided;
- identification of ways to lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- documentation and publication of the outcomes.