London Ambulance Service NHS
NHS Trust

Privacy Impact Assessment Policy for new Processes, Services and Systems

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: Governance and Assurance

Author/Reviewer: IG Manager. To be reviewed by September 2017.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
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**
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 (v2.0)	04/10/16	Governance Administrator	G&A
The Pulse	28/05/12	Governance Co-ordinator	G&C
LA 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	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**

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 Privacy 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 Privacy 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

The Director of Corporate Governance and the Chief Information Officer have strategic responsibility for Information Governance throughout the Trust.

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 **Information Governance Manager**

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

4.5 **Information Security Manager**

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.

4.6 **Information Governance Group**

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

4.7 **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 PIA is undertaken for new processes and projects as required.

4.8 **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 Privacy 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.

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 Mandate.** When completing a Project Mandate the Programme Manager will provide an initial analysis of the implications for Information Governance in order to ensure that there will be no adverse impact on information quality or a breach of information security, confidentiality or Data Protection requirements. The information gathered in this document will also be used to inform the Project Initiation Document.

An initial screening will be carried out in order to determine whether a Privacy Impact Assessment is necessary.

6.3 **Project Initiation Document (PID).** The Project Manager will check what has been identified at the Project Mandate stage 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 Manager to provide advice on appropriate security controls at this stage.

If the outcome of the initial screening indicates that a PIA 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 PIA should be reflected in the document approved by the Project Board.

7. Background to Privacy Impact Assessments (PIAs)

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 Commissioners Office has developed a Privacy Impact Assessment (PIA) Code of Practice 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 Information Governance Toolkit, have identified PIAs 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 PIA 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 PIA. However, a preliminary screening needs to be carried out in order to determine whether a PIA is necessary. The Information Commissioner's Office recommends that PIAs 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.

PIAs 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 PIA should be commenced as part of a project's initiation stage.

PIAs 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 PIA. FAQs are provided in Appendix 4.

The outcomes of the PIA 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 PIA

The following are the main stages of a PIA:

8.1 PIA screening

In order to decide whether a PIA 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 PIA is necessary. The Information Governance Manager must be advised so that the PIA process can be registered and advice and training provided as appropriate. If the completion of the screening questions indicates that no PIA is required the person responsible for undertaking the PIA Initial Assessment should sign the document and send it to the Information Governance Manager.

8.2 The need for a PIA is identified

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

8.3 Step one: The need for a PIA

Explain why the need for a PIA was identified and and the objectives and benefits of the project or initiative.

8.4 Step two: Describing Information Flows

Explain how information will be obtained, used, and retained – explain what information is used, what it is used for, and who will have access to it. This step can be based on, or form part of, a wider project plan. This process can help to identify potential 'function creep' -unforeseen or unintended uses of the data (for example data sharing). The information flows can be recorded in a flowchart or the Information Asset Register. The template at Appendix 2 can be used to record information flows.

8.5 Step three: Identifying Privacy and Related Risks

Record the risks to individuals, including possible intrusions on privacy where appropriate. Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust. Appendix 3 can be used to identify DPA compliance risks. Maintain a record of the identified privacy risks using the template at Appendix 2 if appropriate.

8.6 Step four: Identifying and Evaluating Privacy Solutions

Identify what action could be taken to address risks to privacy. Devise ways to reduce or eliminate privacy risks. Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes. It should be recorded whether each privacy solution that has been identified results in the privacy risks being eliminated, reduced, or simply accepted. The template at Appendix 2 can be used to record the key findings at this stage of the PIA.

8.7 **Step five: Signing Off and Recording the PIA outcomes**
Produce a PIA report which should include an overview of the project, explaining why it was undertaken and how it will impact on privacy. It should include or reference the material which was produced during the PIA, for example the description of data flows and the privacy risk register. The report should describe how the privacy risks were identified and how they will be addressed. Reports for large scale projects should be signed off by a Director or project executive. Smaller scale project reports should be completed by the project manager within the organisation. A copy of the report should be forwarded to the Information Governance Manager and reports will be considered for publication in the Freedom of Information Publication Scheme by the Information Governance Group.

8.8 **Step six: Integrating the PIA Outcomes Back into the Project Plan**
The results of the PIA should be fed back into the wider project management process ensuring that the steps recommended by the PIA are implemented. Continue to use the PIA throughout the project lifecycle when appropriate

IMPLEMENTATION PLAN	
Intended Audience	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.
Dissemination	Available to all staff on the Pulse
Communications	Policy to be announced in the RIB and a link provided to the document
Training	Training will be provided for all staff required to undertake PIAs as part of the Information Governance training programme and advice will be available from the Information Governance Manager.

Monitoring:

Aspect to be monitored	**Frequency of monitoring AND Tool used**	**Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported**	**Committee/ group responsible for monitoring outcomes/ recommendations**	**How learning will take place**
Number of PIAs completed	Quarterly reports	Information Governance Manager to Information Governance Group	Risk Compliance and Assurance Group	Increase profile of PIAs to managers as required

Appendix 1

Privacy impact assessment screening questions

These questions are intended to help decide whether a PIA is necessary.
Answering 'yes' to any of these questions is an indication that a PIA is required.

		Yes/No
1.	**Will the project involve the collection of new information about individuals?**	
2.	**Will the project compel individuals to provide information about themselves?**	
3.	**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**	
4.	**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**	
5.	**Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition**	
6.	**Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?**	
7.	**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 particularly private.**	
8.	**Will the project require you to contact individuals in ways which they may find intrusive?**	

If the answer is 'No' to all of the above questions the person responsible for undertaking the PIA Initial Assessment should sign below and forward to the Information Governance Manager.

Signed……..... Date…….

Name…….

Position……..

Appendix 2

Privacy impact assessment template

This template should be used to record the PIA process and results. Start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Referring to Step three explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Consultation can be used at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
Appendix three can be used to help identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Appendix 3

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
Have you identified the purpose of the project?
How will individuals be told about the use of their personal data?
Do you need to amend your privacy notices?
Have you established which conditions for processing apply?
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
If your organisation is subject to the Human Rights Act, you also need to consider:
Will your actions interfere with the right to privacy under Article 8?
Have you identified the social need and aims of the project?
Are your actions a proportionate response to the social need?

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?
Have potential new purposes been identified as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Is the information you are using of good enough quality for the purposes it is used for?
Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.
If you are procuring new software does it allow you to amend data when necessary?
How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shallnot be kept for longer than necessary for that purpose or those purposes.
What retention periods are suitable for the personal data you will be processing?
Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Will the project require you to transfer data outside of the EEA?
If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 4

FAQs

1. Who should carry out a Privacy Impact Assessment?

Privacy Impact Assessments 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 PIA. It is essential that the person(s) undertaking the PIA 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 Information Governance Manager.

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

The Information Commissioners Office envisages that PIA'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 Privacy Impact Assessment?

The nature of the PIA 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 PIA 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 PIA process.

PIAs 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 PIA as part of the Project Mandate/PID (or its equivalent).

4. What are the benefits of completing Privacy Impact Assessments?

The objective of the PIA 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 PIA 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 PIA 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 PIA 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 PIA 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). The Data Protection Act already stipulates eight Data Protection Principles, but these only address certain aspects of privacy and PIA's can also be taken into account.

5. How do I set up a Privacy Impact Assessment?

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

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

Conducting a PIA usually requires diversity of expertise and interests and PIA's 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 Privacy Impact Assessment?

PIAs 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 PIAs 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 PIA?

Ideally the end results of an effective PIA 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.