London Ambulance Service NHS Trust

Information Governance and Privacy Impact Assessment Policy and Procedure for new Processes, Services and Systems

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To assess 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 and to undertake Privacy Impact Assessments where required.

.

Sponsor Department: Governance and Compliance

Author/Reviewer: IG Manager. To be reviewed by May 2012.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
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**
IGG	27/05/11	1.0
Agreed by Trust Board (If appropriate):		

Published on:	**Date**	**By**	**Dept**
The Pulse			GCT
LAS Website			GCT
Announced on:	**Date**	**By**	**Dept**
The RIB			GCT

EqIA completed on	**By**
28/03/11	C D-B; 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 and procedure 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 and procedure 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 assess 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 introduce Privacy Impact Assessments in the LAS to test that all new projects, processes and systems which are introduced or developed comply with confidentiality, privacy and data protection requirements.

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 Services

The Director of Corporate Services has 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 and procedure supports the Caldicott function.

4.4 **Assistant Director Corporate Services**

The Assistant Director Corporate Services has responsibility for the Governance and Compliance team which includes Information Governance.

4.5 **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 and procedure.

4.6 **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.

4.7 **Information Governance Group**

The Information Governance Group, chaired by the Director of IM&T who is the Senior Information Risk Owner (SIRO), and including the Caldicott Guardian, has strategic responsibility for monitoring the implementation of this policy and procedure, its effectiveness, and acting upon any risks or issues identified.

4.8 **Directors, Senior Managers & IAOs**

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

4.9 **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 minimize privacy concerns.

5.2 Personal Identifiable 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 Trust's Programme and Change Management Office project management process and documentation as follows:

Stage 3: Project Mandate. If completing a Project Mandate an initial analysis of the implications for Information Governance must be considered as detailed in the Project Mandate document.

Stage 5: Project Guidance Information. The Information Governance section outlines the background to the requirement detailed in this Policy and Procedure.

Stage 6: Project Brief. Check what has been identified at Stage 3 if a Project Mandate was completed or if there is no Project Mandate an initial analysis of the implications for Information Governance must be considered at this stage as detailed in the Project Brief document. For example 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 must be documented.

6.2 If the project involves the creation, use or handling of personal identifiable information the project manager should undertake a PIA Initial Assessment as detailed in Section 8.2 below.

6.3 If the outcome of the Initial Assessment indicates that a PIA needs to be carried out it should be completed prior to the project reaching Stage 11 (milestone plan) of the project management process as any changes to the project as a result of undertaking a PIA will need to be incorporated in the plan.

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) framework for organisations to use when developing and introducing projects and processes that may have an impact on how we use patient and staff information. Connecting for Health, via the Information Governance Toolkit, have identified PIAs as a key tool in addressing confidentiality and privacy concerns and they now form part of the Core IG Statement of Compliance requirements for all NHS organizations.

All new or significantly changed processes or projects that involve Person Identifiable 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 evaluation needs to be carried out in order to determine whether a PIA is necessary and, if so, what level of PIA is required. 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 who is familiar with the project should be assigned the responsibility for undertaking the PIA.

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.

7.2 The following are the main stages of a PIA:

7.2.1 **Initial assessment**
Examines the project at an early stage, identifies stakeholders, makes an initial assessment of privacy risk and decides which level of assessment is necessary.

7.2.2 **Full-scale PIA**
Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them. **The documentation is more formalised for a Full- Scale PIA. The template in appendix 6 will provide a useful summary of the documentation created.**

7.2.3 **Small-scale PIA**
Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project. Completion of the template in Appendix 6 will constitute adequate documentation.

7.2.4 **Privacy law compliance check**
Focuses on compliance with various "privacy" laws such as the Human Rights Act 1998 (HRA), Regulation of Investigatory Powers Act 2000 (RIPA) and Privacy and Electronic Communications Regulations 2003 (PECR) as well as the Data Protection Act 1998. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information.

7.2.5 **Data protection compliance check**
Checklist for compliance with DPA. Usually completed when the project is more fully formed.

7.2.6 **Review**

Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should be subject to a PIA.

8. Privacy Impact Assessment Procedure

8.1 A member of the Project Team who is familiar with the project or initiative should be assigned the responsibility for undertaking the PIA as detailed below and in the appendices. This should be a decision of the project board or the relevant department head/ Information Asset Owner should a formal project board not be in existence. The project team or department head must advise the Information Governance Manager so that the PIA process can be registered and advice and training provided as appropriate. The first activity to be carried out is the preparation for the Initial Assessment.

8.2 Initial assessment

Some preliminary work needs to be carried out to determine whether a privacy impact assessment (PIA) needs to be carried out and, if so, what level of PIA is required.
This is a fairly short process but provides a basis for the work required when it comes to actually completing a PIA or checking legal compliance. This preliminary evaluation should be carried out as it can be very expensive to discover too late that a project has substantial privacy impacts. Equally, it would be a waste of resources to unnecessarily carry out a PIA, or complete a full-scale PIA where only a small-scale PIA is needed.

The initial assessment consists of two stages: Preparation and a series of screening questions.

8.2.1 Preparation

Sufficient information must be gathered to allow the questions in the screening process to be applied. It is possible that there will not be enough available information about the project to enable a clear conclusion to be reached in respect of any particular aspect. To help ensure that enough information is available to decide which level of PIA, if any, is required, the following three pieces of information are needed:

a) a project outline;
b) a stakeholder analysis; and
c) an environmental scan.

The screening process questions are likely be answered (at least provisionally) on the basis of this information.

a). Project Outline

During the early stages of a project, there is only limited documentation available, and there may be uncertainty about the project's scope and the features of the intended system. In order to be clear about the project's aims and to start thinking about what the potential impact of the project might be, a copy of the project mandate or project brief will be required. If such documents are not available, consult with relevant staff in the Trust, key stakeholders, members of the project steering committee, and perhaps others as appropriate to the circumstances. From this information, a relatively short description of the project can be prepared if necessary, as a basis for subsequent analysis.

b) Stakeholder Analysis

This involves making a list of any groups or organisations who may have an interest in, a role to play in delivering, or be affected by the project. This could include:

- LAS staff;
- other organisations directly involved in the project;
- organisations and individuals that are intended to benefit from it;
- organisations and individuals that may be affected by it; and
- organisations that provide technology and services to enable it.

At this stage there needs to be as broad a list of groups as possible with a very brief description of the stake each group might have in the project. This list can be edited down later for more focused consultation. At this stage any analysis of stakeholders should be brief, ideally a one page summary.

c) Environmental Scan

It may be valuable to seek out information about prior projects of a similar nature. Where new technology is being used, or the project applies existing technology in new ways, it is likely to assist the evaluation if descriptions of the technology and its applications are gathered.

The following sources may be considered:

- Prior PIAs on similar projects, whether conducted within the LAS, by other organisations or in other countries.
- Fact sheets, white papers, reports and refereed articles published by industry associations, technology providers, and research centres.
- Consultations with professional associations.
- Consultations with privacy regulators, in particular the Information Commissioner's Office.

- Consultations with other regulators.

- Consultations with non-government organisations that represent or provide advice to those potentially affected by the project.

  These investigations may reveal designs and design features that have been devised by other project teams in order to address much the same categories of problem confronted by the project under consideration.

  As with the rest of the preparation work, this does not have to be exhaustively catalogued. A summary with reference to working documents generated during the process should be enough.

8.2.2 Screening Questions

Once the information has been gathered together and the preparatory work has been completed the screening process needs to be carried out. This involves answering the questions set out in Appendix 2 and a flow chart of the screening process is provided at Appendix 1.

The purpose of the screening process is to ensure that the investment the LAS makes is proportionate to the risks involved. Depending on the scope and size of the project, only some elements of this procedure will be relevant in any given case.

Answering these four sets of questions about the project should provide an indication of whether a PIA is needed, and if so, whether the project requires a full-scale PIA.

In addition, the Screening Tool clarifies whether Compliance Checking is necessary against privacy laws generally, and the Data Protection Act specifically.

a) Is a full-scale PIA recommended?

Do the key characteristics of the project indicate that a full-scale PIA is needed? Complete the screening questions in Appendix 2 Step 1.If yes then conduct a full-scale PIA (Appendix 3), a privacy law compliance check (Appendix 5) including data protection compliance check (Appendices 6 and 6.1).If a full-scale PIA is not recommended then:

b) Is a small-scale PIA recommended?

Do the project characteristics indicate that a small-scale PIA is needed? Appendix 4.1 provides some examples. Complete the screening questions in Appendix 2 Step 2. If yes then conduct a small-scale PIA (Appendix 4) and a privacy law compliance check (Appendix 5) including data protection compliance check (Appendices 6 and 6.1).If a small-scale PIA is not recommended then:

c) Is privacy law compliance checking recommended?

Are any of the activities subject to any form of privacy law? If yes then conduct a privacy law compliance check (Appendix 5) including data protection compliance check (Appendices 6 and 6.1).If a privacy law compliance check is not recommended then:

d) Is Data Protection Act compliance checking recommended?

Do the activities involve the handling of 'personal data'? If yes then conduct a data protection compliance check (Appendices 6 and 6.1).

8.3 Further Actions

8.3.1 If the completion of the screening questionnaire 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.

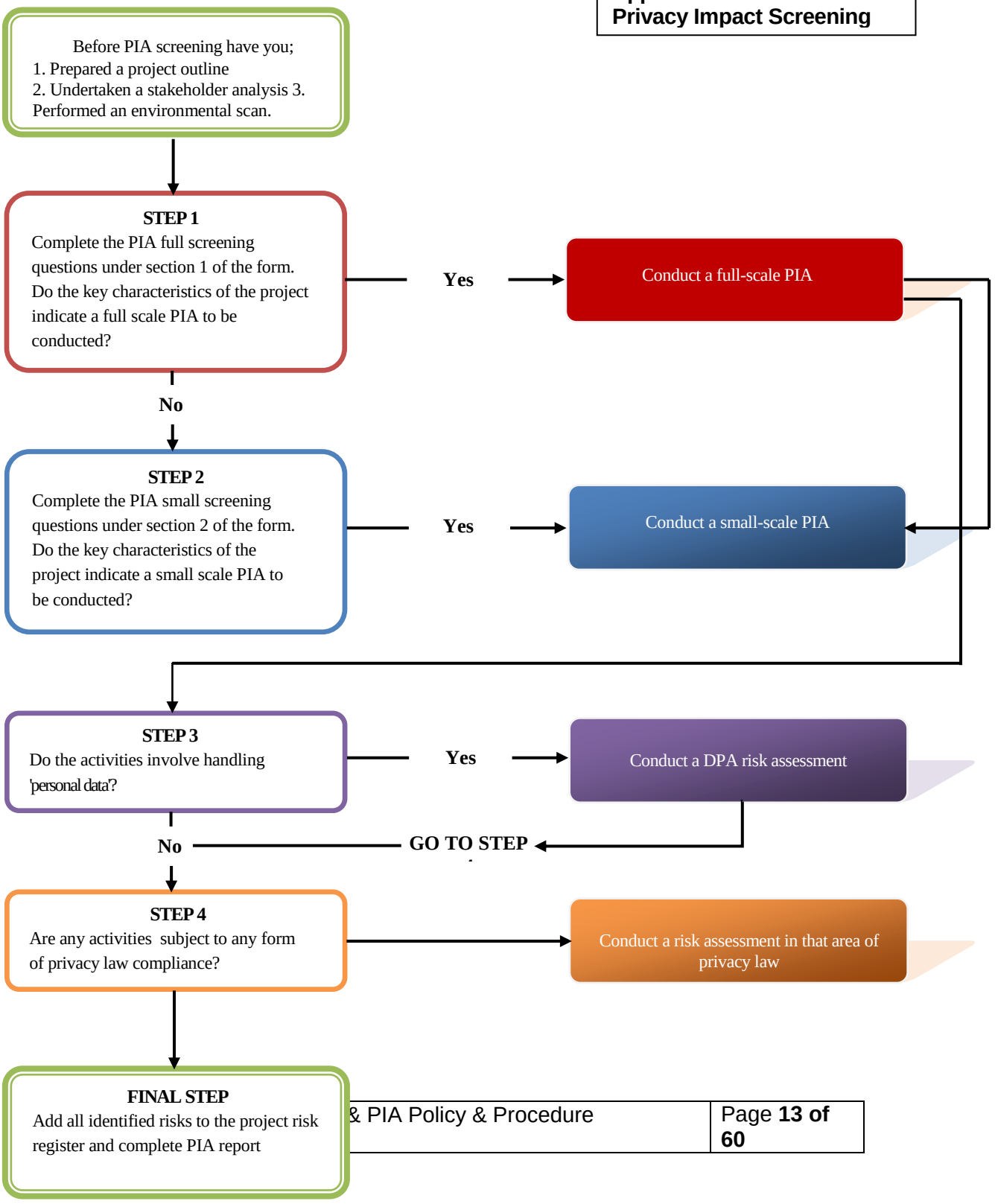
8.3.2 If just a privacy law compliance check and/or Data Protection Act compliance check is undertaken the person responsible for undertaking the PIA should sign the screening questionnaire and send this and evidence of the privacy law compliance check and/or Data Protection Act compliance check (template in Appendix 6.1) to the Information Governance Manager.

8.3.3 If a small-scale PIA is undertaken the person responsible for undertaking the PIA should sign the screening questionnaire and send this and evidence of the small-scale PIA (see Appendix 4 for deliverables) plus the privacy law compliance check, and Data Protection Act compliance check (template in Appendix 6.1) to the Information Governance Manager.

8.3.4 If a full-scale PIA is undertaken the person responsible for undertaking the PIA should sign the screening questionnaire and send this and evidence of the full-scale PIA plus the privacy law compliance check, and Data Protection Act compliance check (template in Appendix 6.1) to the Information Governance Manager. See Appendix 3 for the deliverables for the different stages of a full-scale PIA. The key deliverable of a full-scale PIA is a report that details impacts identified and the solutions or actions that will deal with them.

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 and Procedure 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 Information governance specialists.
Monitoring	Monitoring of this policy and procedure will be through regular reports, including a summary of PIAs undertaken, to the Information Governance Group and an annual review by a member of the Group. Random audits may be undertaken on the application of this policy and procedure to new projects and initiatives.

Appendix 1:
Privacy Impact Screening



Appendix 2

The Privacy Impact Assessment Screening Questionnaire

Project Information	
Project name:	**Date:**
Programme:	

Contact Information	
Name:	
Title:	
Office:	
Phone:	**Fax:**
Email:	

Step 1: Full-Scale Screening Questions				
A: technology				
Ref	**Question**	**Yes**	**No**	**Unknown**
A1	Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?	☐	☐	☐
Notes/ Elaboration/ Comments				

B: Identity				
Ref	**Question**	**Yes**	**No**	**Unknown**
B1	Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management process? e.g. Digital signature initiative, multi-purpose identifier, presentation of identity documents as part of registration scheme	☐	☐	☐
Notes/ Elaboration/ Comments				
B2	Might the project have the effect of denying anonymity and pseudonymity, or converting transaction, identity authentication or identity management process	☐	☐	☐
Notes/ Elaboration/ Comments				

C: Multiple Organisations				
Ref	**Question**	**Yes**	**No**	**Unknown**
C1	Does the project involve multiple organisations, whether they are government agencies, e.g., joined-up government initiative, or private sector organisations, e.g., outsource service providers or business partners.	☐	☐	☐
Notes/ Elaboration/ Comments				

D: Data				
Ref	**Question**	**Yes**	**No**	**Unknown**
D1	Does the project involve new or significantly change handling of personal data that is of particular concern to individuals? e.g., Ethnic origin, religious beliefs, health conditions, financial data, data on vulnerable individuals, data which could enable identity theft.	☐	☐	☐

Notes/ Elaboration/ Comments				
D2	Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database? e.g., Welfare administration, health care, consumer credit, consumer marketing.	☐	☐	☐
Notes/ Elaboration/ Comments				
D3	Does the project involve new or significantly changed handling of personal data about a large number of individuals? e.g., Locate people or builds or enhances profile of these individuals	☐	☐	☐
Notes/ Elaboration/ Comments				
D4	Does the project involved new to significantly changed consolidation, intern-linking, cross-referencing or matching of personal data from multiple sources? e.g., Issues around data quality, diverse meaning of superficially similar data-items, retention on data beyond the very short term.	☐	☐	☐
Notes/ Elaboration/ Comments				

E: Exemptions and Exceptions				
Ref	**Question**	**Yes**	**No**	**Unknown**
E1	Does the project relate to data processing which is in any way exempt from legislative privacy protection? e.g., Law enforcement, national security information systems, where schemes have been negated by legislative exemptions or exceptions	☐	☐	☐
Notes/ Elaboration/ Comments				
E2	Does the project's justification include significant contributions to public security measures? e.g., Measure to address concerns about critical infrastructure and physical safety of the population.	☐	☐	☐
Notes/ Elaboration/				

Comments				
E3	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation? e.g., Sales, exchange, unprotected publication in hard copy or electronically-accessible form, or outsourcing of aspects of the data handling to sub- contractors	☐	☐	☐
Notes/ Elaboration/ Comments				

NOTE: If you have answered YES to any of the above questions you will need to carry out a full-scale PIA (see Appendix X), and a privacy law compliance check including data protection compliance check. If you have answered NO you need to complete Step 2.

Step 2: Small-Scale Screening Questions				
A: technology				
Ref	**Question**	**Yes**	**No**	**Unknown**
A1	Does the project apply new or inherently privacy invasive technologies? e.g., Smartcards, radio frequency identification (RFID) tags, biometrics, locator technologies etc.	☐	☐	☐
Notes/ Elaboration/ Comments				

B: Justification				
Ref	**Question**	**Yes**	**No**	**Unknown**
B1	Is the justification for the new data-handling unclear or unpublished?	☐	☐	☐
Notes/ Elaboration/ Comments				

C: Identity				
Ref	**Question**	**Yes**	**No**	**Unknown**
C1	Does the project involve an additional use of an existing identifier?	☐	☐	☐
Notes/ Elaboration/ Comments				
C2	Does the project involve use of a new identifier for multiple purposes?	☐	☐	☐
Notes/ Elaboration/ Comments				
C3	Does the project involve new or substantially changed identity authentication requirements	☐	☐	☐

	that may be intrusive or onerous?			
Notes/ Elaboration/ Comments				

D: Data				
Ref	**Question**	**Yes**	**No**	**Unknown**
D1	Will the project result in the handling of a significant amount of new data about each person, or significant change in exiting data-handling?	☐	☐	☐
Notes/ Elaboration/ Comments				
D2	Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?	☐	☐	☐
Notes/ Elaboration/ Comments				
D3	Does the project involved new linkage of personal data with data in other collections, or significant change in data linkages?	☐	☐	☐
Notes/ Elaboration/ Comments				

E: Data Handling				
Ref	**Question**	**Yes**	**No**	**Unknown**
E1	Does the project involve new or changed data collection policies or practice that may be unclear or intrusive?	☐	☐	☐
Notes/ Elaboration/ Comments				
E2	Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?	☐	☐	☐
Notes/ Elaboration/ Comments				
E3	Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?	☐	☐	☐
Notes/ Elaboration/ Comments				
E4	Does the project involve new or changed data access or disclosure arrangements that may be unclear or extensive?	☐	☐	☐
Notes/ Elaboration/ Comments				
E5	Does the project involve new or changed data retention arrangements that may be unclear or extensive?	☐	☐	☐
Notes/ Elaboration/				

Comments				
E6	Does the project involve changing the medium of disclosure for publicly available information in such a way that the data become more readily accessible than before?	☐	☐	☐
Notes/ Elaboration/ Comments				

F: Exemptions				
Ref	**Question**	**Yes**	**No**	**Unknown**
F1	Will the project give rise to new or changed data handling that is in any way exempt from legislative privacy protections?	☐	☐	☐
Notes/ Elaboration/ Comments				

General Notes:	

NOTE: If you have answered YES to any of the above questions in Step 2 you will need to carry out a small-scale PIA (see Appendix X), and a privacy law compliance check including data protection compliance check. If you have answered NO you need to complete Steps 3 and 4.

Step 3: Data Protection Act Compliance Screening				
If you answer 'yes' to the following question, complete a Data Protection Act compliance check				
Ref	**Question**	**Yes**	**No**	**Unknown**
1	Does the project involve the handling of any data that is personal data, as that term is used in the Data Protection Act? 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act, s.1).	☐	☐	☐
Notes/ Elaboration/ Comments				

Step 4: Privacy Law Compliance Screening If you answer 'yes' to the following question, complete the Privacy Law compliance check				
Ref	**Question**	**Yes**	**No**	**Unknown**
1	Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulations, other than the Data Protection Act?	☐	☐	☐
	▪ In particular, the following laws and other forms of regulation should be considered:	☐	☐	☐
	▪ The Human Rights Act, in particular Schedule 1,Article 8 (right to respect for private and family life) and Article 14 (prohibition of discrimination).	☐	☐	☐
	▪ The Regulation of Investigatory Powers Act 2000 (RIPA) and Lawful Business Practice Regulations 2000	☐	☐	☐
	▪ The Privacy and Electronic Communications Regulations 2003 (PECR).	☐	☐	☐
	▪ The Data Retention (EC Directive) Regulations 2009.	☐	☐	☐
	▪ In the case of government agencies, the statutes under which the agency or programme operates.	☐	☐	☐
	▪ Statutes that impose regulatory conditions on the manner in which NHS organisations operate.	☐	☐	☐
	▪ Sectoral legislation	☐	☐	☐
	▪ Statutory NHS codes	☐	☐	☐

2	Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy?	☐	☐	☐
	In particular, the following should be considered: confidential data relating to a person, as that term would be understood under the common law of confidence; the tort of privacy as it develops through case law	☐	☐	☐
3	Does the project involve any activities (including any data handling) that are subject to less formal good practice requirements relevant to privacy?	☐	☐	☐
	In particular, the following should be considered: industry standards, e. g., the BS ISO / IEC 17799:2005	☐	☐	☐
	Information Security Standard; the NHS Confidentiality Code of Practice	☐	☐	☐
Notes/ Elaboration/ Comments				

Completed by_____ Date_____

Appendix 3

Full-Scale PIA

The five stages of a full-scale PIA

1. Preliminary phase.
2. Preparation phase.
3. Consultation and analysis phase.
4. Documentation phase.
5. Review and audit phase.

1. Preliminary phase

This is phase one of the five-phase PIA process.
The purpose of this phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently. **The suggested deliverables are a project plan and a project background paper.**

The following tasks are suggested:

- Review the outcomes and documents from the initial assessment. If necessary, prepare any documents that were not produced during the initial assessment and which might be helpful in completing the PIA.

- Develop the project outline produced in the initial phase.

- Ensure at this stage that the terms of reference, the scope and the resources dedicated to the PIA are appropriate.

- Hold preliminary discussions with relevant organisations. These discussions would generally focus on relevant parts of the organisation itself and any key participating organisations. Early discussions with external organisations, including the Information Commissioner's Office, may also be advisable in some circumstances.

- Hold preliminary discussions with representatives of and advocates for stakeholder groups. This is likely to be of importance where particular external parties may be significantly affected by the project and what it delivers.

- Conduct a preliminary analysis of privacy issues. This is likely to commence with a deeper re-consideration of the outcomes of the screening process.

- Prepare the project background paper. This document will establish the basis for discussions with stakeholders.

Developing the project outline

An outline or background paper for the project that is subject to the PIA will have been obtained or produced. The preliminary phase of the five-phase PIA process leads to the development of this project background paper. The following provides guidance in relation to its content.

The purpose of the project background paper is to establish a sound base for the subsequent preparation, consultation and analysis. The project background paper should contain the following, many of which will already exist in some form.

- A description of the context or setting in which the proposal is being brought forward (including relevant social, economic and technological considerations).

- A statement of the motivations, drivers or opportunities underlying the project.

- A statement of the project's objectives, scope and business rationale.

- A description of the project's design reflecting the Trust's current understanding of how the project will take shape. The explanation needs to be at a sufficient level of detail that participants can consider the project's impacts and implications. The detail available will vary depending on the developmental stage of the project. The design description may be conceptual and sketchy if salient design features have not been pre-determined. If the project has already been through the requirements analysis and design phases, the project background paper can describe the flows of personal information at the appropriate level of detail. These may be placed in appendices containing diagrams that depict process descriptions and lists of items of personal data involved.

- An initial assessment of potential privacy issues and risks, including both obvious or direct impacts and longer-term or secondary impacts on privacy, as perceived by the LAS at the time the document is prepared.

- Brief descriptions of options and sub-options that the lead organisation has identified, including both those already dismissed, and those that remain under consideration.

- The business case which explains the justification for the features that give rise to the potential impacts on privacy, expressed both as:

    - an explanation of how the key features of the scheme will achieve the objectives; and

    - a cost / benefit analysis.

- Descriptions of the project plan as a whole, the PIA process within it, and the consultation processes within the PIA.
- Lists of involved organisations, stakeholder groups and representatives and advocates who have been or will be invited to contribute to the PIA.

- Attachments, as appropriate, that will contribute to understanding the project and its potential privacy implications.

The project background paper should contain a clear and well-argued case for the project as a whole, and particularly for those features that have greatest potential for negative privacy impacts. This will help the identification and collaborative examination of privacy risks and, ultimately, in having an effective PIA.

This process of rigorous challenge and justification for privacy-intrusive aspects of schemes should be continued through logical design, to physical design, construction and integration, and on to implementation. This process facilitates the discovery of alternatives to achieve project goals while minimising negative impacts, and the creation of compensating measures to address project features with negative impacts that are judged to be necessary despite their downsides.
Where some of the information is subject to commercial or security sensitivity, that information can be separated into an appendix, which can be distributed less widely and/ or subject to clear confidentiality constraints. This enables the issue to be managed without compromising
the openness of the bulk of the information.

There may be some resistance to providing some of this information to stakeholders. For example, designers may consider that hey do not need to give any explanations of the reasons for aspects of the concept or the design that some stakeholders may see as privacy-threatening. The project manager may hesitate to make available the business case underlying particular features or even the project as a whole. This may be in part for understandable commercial or security reasons. On the other hand stakeholder trust needs to be achieved. It is important that information is not withheld because it exposes poor thinking.

Where elements of the document cannot be delivered at the outset, it may be appropriate to distribute the information in two or more instalments. Additional information may be needed in the case of projects that involve technologies that are new, or are otherwise unlikely to be understood by the participants in the consultation process.

To achieve an effective consultation process, the primary sponsor may need to make available technical documentation and briefings, and perhaps demonstrations. Examples of technologies for which this is currently likely to be needed include:

- contact-based smartcards;
- contactless smartcards and RFID tags;
- identity management;
- portals for services and authentication;
- data warehousing and data mining;

- locator technologies; and
- biometrics.

2. Preparation phase

This is phase two of the five-phase PIA process.

The purpose of this phase is to make the arrangements needed to enable the critical phase three to run smoothly.

The suggested deliverables are a stakeholder analysis, a consultation strategy and plan, and the establishment of a PIA consultative group (PCG). The following tasks are suggested:

- Develop a consultation plan to ensure that discussions with stakeholders are effective.
- Form a PIA consultative group (PCG). This comprises representatives of stakeholder groups.
- Distribute the project background paper to the PCG. This ensures that the PCG members can understand the nature of the proposal.

Developing a consultation plan

Any project that is sufficiently complex and potentially privacy-threatening that it requires a full-scale PIA is likely to affect many parties. To ensure the most is made of the consultation and analysis phase, it is useful to put a consultation plan in place. Remember that any consultation should be appropriate to the scale, scope and nature of the project for which a PIA is being completed. Large-scale projects that embody significant privacy risks, might use most or all of the methods described below. In small-scale projects it may not be necessary to use all of these. A well-developed consultation strategy may already be in place and there is no reason why any PIA consultation cannot be completed within this strategy. If a consultation strategy is not in place, further advice is provided below.

Effective consultation depends on all stakeholders being sufficiently well-informed about the project, having the opportunity to convey their perspectives and their concerns, and developing confidence that their perspectives are being reflected in the design.

It is common for consultation processes to result in changes to the project and to its design. In order to make the maximum contribution to risk management in return for the smallest cost, consultation therefore needs to commence early and continue throughout the project life-cycle. Some useful ways of ensuring effective consultation include:

- priming of discussions by providing some initial information about the project;

- making sure there is ongoing dialogue with consultees throughout the PIA process;

- participation of representatives of, and advocates for, stakeholder groups who have appropriate background in the technologies, systems and privacy impacts involved;

- facilitated interactions among the participants;

- making sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered;

- making sure that each group has the opportunity to provideinformation and comment, even including multiple rounds of consultation where necessary;

- making sure that the method of consultation suits the consultation group, for example using workshops or focus groups as an alternative to, or even as well as, formal written consultation;

- making sure that the information provided by all parties to the consultation is fed into the subsequent rounds of design and implementation activities; and

- ensuring that the perspectives, concerns and issues raised during the consultation process are seen to be reflected in the outcomes of the PIA process.

Devise communication processes that will enable the effective interchange of ideas. This may involve workshops and meetings, perhaps supplemented by formal submissions.

Where security considerations or indeed other privacy concerns prevent the consultation processes from being fully open, it is suggested that:

- the PIA be undertaken in as open a manner as is possible;

- parts which have security concerns be separated into closed or confidential appendices and separate, relatively closed discussion sessions; and

- where security considerations result in the suppression of information, proxy measures be devised that are as effective and credible as possible. (For example, the security-sensitive information could be provided to a trusted third party who could then deliver to PCG members evaluative comments that avoid exposing the information).

3. Consultation and analysis phase(s)
This is phase three of the five-phase PIA process.

It involves consultations with stakeholders, risk analysis, and identification of problems and the search for solutions. The purpose of this phase is to ensure that problems are identified early, that effective solutions are found and that the design is adapted to include those solutions. **The suggested deliverables are changes to the project documents, an issues register, and a privacy design features paper.** The following tasks are suggested:

- Implement the consultation plan that was established during the previous phase.

- Identify the design issues and privacy problems with the project.

- Re-consider the design options. This focuses on the various approaches that are available to solve problems.

- Document the problems and solutions in an 'issues register'. There is a risk with large projects that corporate memory will be lost if the PIA is carried out in stages. This problem can be overcome by carrying the issues register forward as an appendix to each revision of the project background paper that is made available to the PCG. The issues register also serves as a means to note issues that cannot be addressed immediately and avoid the possibility of them being overlooked.

- Reflect the conclusions reached, in the issues register and/ or in an evolving 'privacy design features paper'. This documents:

    - issues identified;
    - avoidance and reduction measures considered and either rejected or adopted;
    - design changes to be undertaken as a result; and
    - outstanding issues.

- Provide the privacy design features paper to:

    - the PCG; and
    - the project team.

- Pass the project team's feedback to the PCG.

- Conduct further consultations with the PCG.

- Incorporate the decisions on privacy design features into the design.

- Where there are unresolved issues, continue consultation and analysis.

This phase generally involves repeating the exercise a number of times. The most effective approach is to conduct the exercise first at the stage of project initiation, and arrange subsequent run-throughs to correspond with the later phases of the project, e. g., requirements analysis, logical design, physical design, construction, integration and deployment of the new system.

The project background paper is likely to require progressive changes to reflect developments during the project. As will be apparent from the descriptions provided, it is normal for a PIA to result in changes to the design in order to reduce or avoid privacy intrusion. Late changes can of course be expensive. This is an important reason why early commencement of a PIA is recommended.

4. Documentation phase

This is phase four of the five-phase PIA process.

A privacy impact assessment is a process. The benefits arise mainly from that process, in the form of learning and adaptation, partly by the stakeholders, and partly by the LAS and the team responsible for the project.

There are, however, advantages in generating a final document towards the end of the PIA process. The purpose of this phase is to document the PIA process and the outcomes. The suggested deliverable is a PIA report.

The following tasks are suggested:

- Consolidate the decisions on avoidance and mitigation measures into a final version of the issues register and/ or privacy design features paper.
- Produce a PIA report.
- Make the PIA report available to the PCG.
- Publish the PIA report (withholding any security-sensitive information in confidential, or closed, appendices).

The reasons for preparation of a PIA report are:

- as an element of accountability, in order to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit;
- to provide corporate memory, ensuring that the experience gained during the project is available to those completing new PIAs if original staff have left; and
- to enable the experience gained during the project to be shared with future PIA teams and others outside the LAS.

The following are key elements of a PIA report:

- A description of the project.

- An analysis of the privacy issues arising from it.
- The business case justifying privacy intrusion and its implications.
- Discussion of alternatives considered and the rationale for the decisions made.
- A description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features.
- An analysis of the public acceptability of the scheme and its applications.

Possible sources for the content of the PIA report include:

- A summary of the consultative processes undertaken
- Contact details of organisations and individuals with whom consultations were undertaken.
- The project background paper(s) provided to those consulted.
- The PIA project plan.
- The issues register and/ or privacy design features paper(s).
- References to relevant laws, codes and guidelines.

At a late stage, once the design has been checked for legal compliance, it may be appropriate to add the following as appendices to the PIA report:

- the Privacy law compliance study; and
- the Data Protection Act compliance study.

A PIA report should be written with the expectation that it will be published, or at least be widely distributed. If so, the report can fulfil the functions listed above: accountability, post-implementation review, audit, input into future iterations of the PIA, and background information for people conducting PIAs in the future.

Some of the information gathered during a PIA process may be subject to security or commercial sensitivities. In such cases, it may be appropriate for the detailed information to be in confidential, or closed, appendices. Such information suppression, however, needs to be limited to only that which is justified. Sufficient information needs to be included within the PIA report to ensure that the arguments and assessments are complete, informative and comprehensible.

5. Review and audit phase

This is phase five of the five-phase PIA process.

The purpose of this phase is to ensure that the undertakings arising from the consultation and analysis phase are carried through into the running system or implemented project.

The following tasks are suggested:

- Undertake a review of the implementation of the mitigation and avoidance measures that were documented in the issues register and/ or the privacy design features paper.
- Prepare a review report.

- Present the privacy review report to the PCG.

- Make the privacy review report publicly available.

As with the preceding phases, it is beneficial to perform this phase at the appropriate stage in the life-cycle of the overall project. This could be, for example, at a milestone such as the detailed design review, or its equivalent in the project method.

Another approach that may be considered appropriate or cost-effective is to build the review of performance into standard, periodic or occasional internal audit or external audit processes

Appendix 4

Small – Scale PIA

Overview

Projects with potentially substantial privacy impacts warrant a full-scale Privacy Impact Assessment (PIA) process. Other projects require attention, but do not warrant as great an investment of time and resources. A small-scale PIA involves analysis of the privacy issues arising from the aspect or aspects that the screening process in Appendix 2 has highlighted through the application of the criteria for small-scale PIA.
A small-scale PIA process differs considerably from a full-scale PIA. In particular:

- it is less formalised;
- it involves less investment;
- it calls for less exhaustive analysis and information-gathering, and
- it is more likely to be focused on specific aspects of a large-scale project rather than the project as a whole.

Because projects vary greatly, a process should be devised that fits the need, is as comprehensive as it needs to be, but is only as resource-intensive as is appropriate in the circumstances. This part draws on the full-scale privacy impact assessment process described in Appendix 3, but is much briefer. The guidance is in two parts:

Background information intended to assist the LAS to gain an appreciation of the kinds of projects for which a small-scale PIA is appropriate, and its key characteristics. Examples are given in Appendix 4.1.

The PIA process: See below.

Why do a small-scale PIA?

The scope of the PIA should reflect the nature of the project as a whole. By conducting a full-scale privacy impact assessment on every project, regardless of its nature, scale or scope, the LAS may be committing too much resource for a project of limited scale or scope. This may lead to the PIA process being perceived as not delivering value.

There is also a danger that too much full-scale public consultation may lead to fatigue among stakeholder groups, who themselves do not have the resources to devote to providing so many consultation responses. As a result, stakeholders may begin to channel resources into higher profile projects. This can lead to the PIA process not achieving one of its core aims of representing the privacy concerns from all perspectives, particularly in more limited projects.

A small scale PIA can be more readily scaled to fit the scale, scope and nature of a smaller project and will require less investment by the LAS.

The small-scale PIA process
The process for completing a small scale PIA for any particular project needs to reflect:

- the nature of the project (eg new system, replacement system, enhancements to an existing system, new technology, outsourcing, changed business processes or staff instructions, replacement user interface, revised privacy policy statement, drafting of legislative changes);

- the specific aspects of the project that the screening process has highlighted;

- any relevant PIAs that have been previously conducted;

- the organisation's level of experience in conducting PIAs.

Conventional project management techniques may be applied to the process of assessing privacy impact.

The phases for a small-scale PIA mirror the detailed guidance for the relevant phase of a full-scale PIA. In a small-scale PIA it may be appropriate to compress phases together, consolidate tasks, or reduce the number of deliverables by merging several documents into one.

The following suggested phases are described below:

1. preliminary phase;

2. preparation phase;

3. consultation and analysis phase(s);

4. documentation phase;

5. review and audit phase.

1. Preliminary phase

The purpose of the preliminary phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently. Depending on the scale of the project and the experience of the project manager in relation to PIAs, it may be appropriate to produce and maintain a project plan. It will generally be advisable to produce or get hold of a project background paper, although this is likely to be quite short.

Because the circumstances in which a small-scale PIA should be conducted vary so much, this Appendix does not contain any specific guidance in relation to this phase,

but a useful checklist is available, which describes the tasks involved in the corresponding phase of full-scale PIAs in Appendix 3. Carrying out all the tasks recommended in the checklist would be excessive for a small project but the ideas can be of assistance, and may be applied in a less onerous manner such as in combination or selectively according to the circumstances.

At the very least, the preliminary phase should have as deliverables a project outline, a preliminary assessment of privacy concerns and some preliminary talks with key stakeholders. A clear and informative project outline will make the consultation and analysis phase much easier and more effective.

2. Preparation phase

The purpose of the preparation phase is to make the arrangements needed to enable the critical phase three to run smoothly. In this phase, a stakeholder analysis may be undertaken, development of a consultation strategy and plan, and establishment of a PIA consultative group (PCG). Due to the nature of a small-scale PIA, these tasks do not need to be formalised.

It will be useful to consult the checklist which describes the tasks involved in the corresponding phase of full-scale PIAs in Appendix 3. It is likely that not every task will be appropriate to a small-scale PIA or that some of the tasks completed as part of a full-scale PIA will need to be scaled back in order to be appropriate to a small-scale PIA.

3. Consultation and analysis phase(s)

The consultation and analysis phase builds on the foundations established by the first two sections. It includes consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

Consultation 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. It may, depending on the size of the project, be limited to a meeting or workshop with the key stakeholders, a series of short telephone interviews or even involve simply writing to the key stakeholders.

Sometimes, projects and systems may develop during the PIA process, in particular where concerns have been raised by stakeholders. As such, it can sometimes be useful to carry out several consultations over time to update stakeholders on developments and ask for further feedback as to whether this has addressed their concerns. On the other hand, if a comprehensive and clear project background paper is produced, and the participants are experienced or issues relatively simple, it may be sufficient to carry out one consultation exercise.

The key deliverable is a document (such as a privacy design features paper or a meeting outcomes report) that details the privacy impacts identified and the solutions or actions which will be taken to deal with them. This document must be in a form which can be published and provided to the various parties involved in the consultation. The project team, and in particular the designers, should receive copies

of this document, because they will need to make decisions based on the outcome of consultations, make changes to the relevant project documents and implement the decisions made.

Again, the corresponding guidance for the consultation and analysis phase as part of a full-scale PIA described in Appendix 3 provides a list of tasks which can be scaled back as appropriate for a small-scale PIA.

4. Documentation phase

The documentation of a full-scale PIA will justify more extensive documentation than a small-scale PIA. The purpose of the documentation phase is to document the process and the outcomes. **The deliverable is a PIA Report**, which may draw heavily on the document produced during the consultation and analysis phase. Depending on the context, this might be a relatively brief 'note to file', with copies to relevant parties; but circumstances may justify a more carefully prepared document.

5. Review and audit phase

The purpose of this phase is to ensure that the design features arising from the PIA are implemented, and are effective. **The deliverable is a review or update report**. Once again, in some contexts a 'note to file', with copies distributed to relevant parties, might be sufficient to achieve this requirement. In other cases, a more detailed document may be required.

Appendix 4.1

Small Scale PIA Project Examples

The following are examples of a range of different kinds of projects for which a small-scale PIA is more likely to be appropriate:

- Replacement of an existing personal data system by new packaged software, with consequential changes to business processes and perhaps data storage.

- Design and development of a new personal data system that will only contain data about people who have given their consent.

- Enhancements to an existing system in order to collect, store and use several additional items of personal data.

- A proposal to collect items of personal data from a new source, e.g. to reduce the costs incurred by the LAS or the inconvenience to the individuals concerned, or to enable cross-checking against data provided by the data subject.

- Revisions to staff instructions relating to the disclosure of personal data.

- Adaptations to an existing system to reflect new legislation, codes or industry standards.

- The application of a new technology to an existing purpose (e.g., replacement of bar-code or magnetic-stripe technology with a contact-based chip containing the same data).

- The re-design of web-forms for capture of personal data from customers, including the explanations provided, and the circumstances in which particular data-items are declared to be mandatory or optional.

- Plans to outsource business processes involving personal data, or the storage and processing of personal data.

- The application of existing personal data to a new purpose.

- Changes to retention policies relating to personal data.

- Policy statements concerning staff usage of employer-provided facilities such as telephones, mobile phones, desktops, portables, and broadband and wireless ISP subscriptions.

- Review of the means whereby patients express their requests, consents and
- denials regarding the disclosure of their medical data from the records of a health care professional or clinic.

- The design of a pseudonymous scheme for customer survey data.

Appendix 5

Privacy law and other legal compliance checking

The importance of compliance checking

The LAS must ensure that the project, the personal data that it handles, and the business processes it uses are compliant with all relevant laws. Compliance checking should be started at an early stage of the project to address issues such as the legality of any proposed course of action, but this work will normally only be completed later, once the design of the project has reached a more detailed stage.

While compliance checking as part of a privacy impact assessment (PIA) will focus on laws which affect privacy, the LAS will have to consider broader legal compliance as well. For example public sector organisations will have to consider the extent of their powers, any obligations they have in relation to the personal information they collect and any prohibitions on the use of that information.

Further documents may be relevant, such as codes of conduct and privacy policy statements, particularly where the LAS has provided some form of undertaking to comply with them. This might arise from membership of an association that issues the code, or the terms of a document that we have produced. There are also matters of public policy that may not be formally law, but that are generally respected.

Appendix 6 provides guidance in relation to compliance with the Data Protection Act. This Appendix relates to broader elements of the law but any legal compliance checking should include these areas.

Responsibilities

The LAS is responsible for undertaking a survey of the law relevant to the project and to the data processing and business processes it gives rise to. All participating organisations should do the same in connection with their involvement in the project.

Information Governance specialists and/or the Legal team should be consulted as part of checking compliance with privacy law and other legal obligations as the compliance checking process needs to take full account of privacy law obligations.

Potentially relevant sources of the law

The following is an indicative, but not exhaustive, list of laws that may be relevant.

- Statutes regulating such activities as public health, education, family law, children's safety, occupational health and safety, archives, telecommunications, and surveillance devices.

- Provisions within the statutes that govern LAS activities and programmes.

- The law of confidence, which has also developed into the tort of misuse of private information.

- The tort of negligence.

- The tort of passing off.

- The Human Rights Act 1998.

Postponing or redesigning a project

To the extent that the design is not compliant with the law, or it would be illegal to deploy the new or adapted system or scheme, it may be necessary to change the design prior to deployment, in order to achieve compliance.

Appendix 6

Data Protection Compliance Check

The role of compliance checking

The LAS must ensure that the project, the personal data that it handles, and its business activities, are compliant with:

- the Data Protection Act (DPA) in general;
- the data protection principles;
- the interpretations of the principles;
- any delegated legislation, such as the Privacy and Electronic Communications Regulations (PECR).

Compliance checking

The LAS must evaluate the project process and the resulting design, in order to ensure that it is compliant with the Data Protection Act. Unlike a Privacy Impact assessment (PIA), which is best commenced early in the project life-cycle, compliance checking is normally conducted later, once the design has reached a detailed stage.

Activities that will be undertaken as part of the resulting system or scheme must be evaluated in order to ensure that they are compliant with the Data Protection Act.

A detailed template is provided in Appendix 6.1 to assist in checking the compliance of a design against the data protection principles. This template is not a comprehensive compliance tool in itself, but does point to the issues that need to be addressed as part of the Trust's compliance checking procedures. It can be a useful starting point for developing in-house compliance checking procedures or quality assuring existing compliance tools that we already have in place.

Postponing or redesigning a project

To the extent that the design is not compliant with data protection law, it may be necessary to change the design prior to deployment, in order to achieve compliance.

Data Protection Compliance Check Template

This checklist aims to assist the LAS to investigate whether the personal information aspects of a project comply with the Principles in Schedule 1 of the Data Protection Act (DPA).

It has been designed as a template to be used by any employee proposing change.

It should be noted that many terms used in the Schedule 1 Principles have meanings specific to the Data Protection Act, and it would be prudent to refer to the Act for definition for those terms. Another useful reference in this regard is the Information Commissioner's Legal Guidance. Users are also encouraged to seek guidance from LAS Information Governance specialists.

I BASIC INFORMATION – New or existing Project, System, Technology or Legislation

1. Organisation and Project

Organisation
Dept / Directorate
Project

2. Contact Position and/or Name, Telephone Number and Email Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name, Title
Dept/ Directorate
Phone Number
E-Mail

3. Description of the Programme / System / Technology /Legislation (Initiative) being assessed.

(Please note here if the initiative does **not** collect, use or disclose personal data). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

4. Purpose / Objectives of the initiative (if statutory, provide citation).

5. What are the potential privacy impacts of this proposal?

6. Provide details of any previous PIA or other form of personal data* assessment done on this initiative (in whole or in part).

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO III DPACOMPLIANCE – CONCLUSIONS

***IMPORTANT NOTE:**
'Personal data' means data which relate to a living individual who can be identified:
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
(Data Protection Act, section 1)

II DATA PROTECTION PRINCIPLES (DPPs)

1 Principle 1: Fair and Lawful Processing

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
For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 19-35

1.1 Preliminary
1.1.1 What type of personal data are you processing?

Please give examples of any sensitive personal data that you are processing.

1.1.2 Are sensitive personal data being differentiated from other forms of personal data?

Yes No

If yes, please specify procedures. If no, please indicate why not.

1.2 Schedule 2 - Grounds for Legitimate Processing of Any Personal Data
1.2.1 Have you identified all the categories of personal data that you will be processing and how?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.2 Have you identified the purposes for which you will be processing personal data and how?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.3 Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.4 Are you relying on different grounds for different categories of personal data?

Yes No

If yes, how will this assessment be made?

1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data
If this project does not involve the processing of sensitive personal data please go to section 1.4

1.3.1 Have you identified the categories of sensitive personal data that you will be processing?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.2 Have you identified the purposes for which you will be processing sensitive personal data?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.3 Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.4 Are you relying on different grounds for different categories of sensitive personal data?

Yes No

If so, how will this assessment be made?

1.4 Obtaining consent

1.4.1 Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?

Yes No

If yes, when and how will that consent obtained?

1.4.2 For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act?

Yes No

If so, when and how will that consent obtained?

1.5 Lawful Processing

a. If you are a public sector organisation:

1.5.1 Does your processing of personal data fall within your statutory powers?

Yes No

If yes, please state what they will be. If no, please indicate why not.

1.5.2 How is compliance with the Human Rights Act being assessed?

b. All organisations:

1.5.3 Are you assessing whether any of the personal data being processed is held under a duty of confidentiality?

Yes No

If yes, how will that assessment made? If no, please indicate why not.

1.5.4 How is that confidentiality maintained? (eg instructions on disclosure or shredding)

1.5.5 Are you assessing whether your processing is subject to any other legal or regulatory duties?

Yes No

If yes, how is that assessment being made? If no, please indicate why not.

1.5.6 How are you ensuring that those legal duties are being complied with?

1.6 Fair Processing

1.6.1 Are individuals being made aware of the identity of your organisation as the data controller?

Yes No

If yes, state how they are being made aware. If no, please indicate why not.

1.6.2 How are individuals being made aware of how their personal data is being used?

1.6.3 How are individuals offered the opportunity to restrict processing for other purposes?

When is that opportunity offered?

1.6.4 Do you receive information about individuals from third parties?

Yes No

If yes, please give examples. If no, please go to section 1.7

1.6.5 How are individuals informed that the data controller is holding personal data about them?

When are individuals informed?

1.7 Exemptions from the First Data Protection Principle

The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair Data Protection Act, Schedule 1, Part II, para. 2 (3)

1.7.1 Do you provide individuals with all of the information in the box above?

If no, which exemption to these provisions is being relied upon?

2 Principle 2: Purpose Limitation

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. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 35-6

2.1 Uses of Personal Data within the Organisation

2.1.1 Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?

Yes No

2.1.2 How often is this record checked?

2.1.3 Does the record cover processing carried out on your behalf (eg by a subcontractor)?

Yes No

2.1.4 What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data?

(Cross reference with section 1.6, Fair Processing)

2.2 Use of Existing Personal Data for New Purposes

2.2.1 Does the project involve the use of existing personal data for new purposes?

Yes No

If no, go to section 2.3

2.2.2 How is the use of existing personal data for new purposes being communicated to:

(a) the data subject;

(b) the person responsible for Notification within the organisation

(c) the Information Commissioner?

2.2.3 What checks are being made to ensure that further processing is not incompatible with its original purpose?

2.3 Disclosures of Data

2.3.1 Do you have a policy on disclosures of personal data within your organisation / to third parties?

Yes No

Is it documented?

Yes No

2.3.2 How are staff made aware of this policy / instructed to make disclosures?

2.3.3 How are individuals / data subjects made aware of disclosures of their personal data?

2.3.4 Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed?

Yes No

If no, go to section 3.1

If yes, how do you make the assessment?

3 Principle 3: Adequate, Relevant and Not Excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 36-37

3.1 Adequacy and relevance of Personal Data

3.1.1 How is the adequacy of personal data for each purpose determined? (Please give examples.)

3.1.2 How is an assessment made as to the relevance (ie no more than the minimum required) of personal data for the purpose for which it is collected?

3.1.3 What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?

How often will these procedures reviewed?

3.1.4 Are there procedures for assessing the amount and type of personal data collected for a particular purpose?

Yes No

If yes, please describe. If no, please indicate why not.

3.1.5 Are items of personal data held in every case which are only relevant to a subset of those cases?

Yes No

4 Principle 4: Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 37-8

4.1 Accuracy of Personal Data

4.1.1 Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?
Yes No

4.1.2 How, and how often, are personal data be checked for accuracy?

Please give examples:

4.1.3 In what circumstances is the accuracy of the personal data being checked with the Data Subject?

Please give examples:

4.1.4 Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record?

Yes No

If so, how? Please give examples:

4.1.5 Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate?

Yes No

If no, please indicate why not.

4.2 Keeping Personal Data Up to Date

4.2.1 Are there procedures to determine when and how often personal data requires updating?

4.2.2 Are personal data evaluated to establish the degree of damage to:
(a) the data subject
Or

(b) the data controller

that could be caused through being out of date?

Yes No

Please specify whether to data subject or data controller:

4.2.3 Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?

Yes No

5 Principle 5: No Longer than Necessary

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance p 39

5.1 Retention Policy
5.1.1 What are the criteria for determining retention periods of personal data?

How often are these criteria reviewed?

5.1.2 Does the project(s) include the facility to set retention periods?

Yes No

5.1.3 Is the project subject to any statutory / sectoral requirements on retention?

Yes No

If yes, please state relevant requirements:

5.2 Review and Deletion of Personal Data
5.2.1 Is there a review policy?
Yes No

Is it documented?

Yes No

5.2.2 When data is no longer necessary for the purposes for which it was collected:

(a) How is a review made to determine whether the data should be deleted?

(b) How often is the review to be conducted?

(c) Who is responsible for determining the review?

(d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?

Yes No

5.2.3 Are there be any exceptional circumstances for retaining certain data for longer than the normal period?

Yes No

If yes, please give justification:

5.2.4 Is there any guidance on deletion / destruction of personal data?

Yes No

If no, please indicate why not.

6 Principle 6: Data subject access

Personal data shall be processed in accordance with the rights of data subjects under this Act. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 39-40

6.1 Subject Access

6.1.1 Are procedures in place to provide access to records under this Principle?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.1.2 How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?

6.1.3 Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject?

Yes No

If yes, how? If no, please indicate why not.

6.1.4 Are procedures in place to manage personal data relating to third parties?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.1.5 How is data relating to third parties managed?

6.2 Withholding of personal data in response to a subject access request

6.2.1 Are there any circumstances where you would withhold personal data from a subject access request?

Yes No

If no, go to section 6.3. If yes, on what grounds?

6.2.2 How are the grounds for doing so identified?

6.3 Processing that may cause Damage or Distress

6.3.1 Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.3.2 Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?

Yes No

6.4 Right to Object

6.4.1 Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?

Yes No

6.5 Automated Decision-Taking

6.5.1 Are any decisions affecting individuals made solely on processing by automatic means?

Yes No

If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?

6.6 Rectification, Blocking, Erasure and Destruction

6.6.1 What is the procedure for responding data subject's notice (in respect of accessible records) or a court order requiring:

(a) rectification;

(b) blocking;

(c) erasure or;

(d) destruction of personal data?

7 Principle 7: Data Security

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. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 40-3

7.1 Security Policy

7.1.1 Is there a Data Security Policy?

Yes No

If no, please indicate why not and then go to 7.1, question 5.

7.1.2 If yes, who / which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?

7.1.3 Does the Data Security Policy specifically address data protection issues?

Yes No

7.1.4 What are the procedures for monitoring compliance with the Data Security Policy within the organisation?

7.1.5 Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?

7.1.6 Is the level of security appropriate for the type of personal data processed?

7.1.7 How does the level of security compare to industry standards, if any?

7.2 Unauthorised or unlawful processing of data

7.2.1 Describe security measures that are in place to prevent any unauthorised or unlawful processing of:

(a) Data held in an automated format (eg password controlled access to PCs)

(b) Data held in a manual record (eg locked filing cabinets)?

7.2.2 Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing?

Yes No

If yes, please describe the planned procedures. If no, please indicate why not.

7.2.3 Describe the procedures in place to detect breaches of security (remote, physical or logical)?

7.4 Destruction of Personal Data
Cross-reference with section 5.2

7.4.1 Describe the procedures in place to ensure the destruction of personal data no longer necessary?

7.4.2 Are there different procedures for destroying sensitive personal data?

Yes No

7.5 Contingency Planning - Accidental loss, destruction,damage to personal data
7.5.1 Is there a contingency plan to manage the effect(s) of an unforeseen event?

Yes No

7.5.2 Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through:

- human error
- computer virus
- network failure

- theft
- fire
- flood
- other disaster.

8. Principle 8: Overseas Transfer

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. For the Information Commissioner's guidance in relation to this Legal Guidance DPP, see pp 43-5

8.1 Adequate Levels of Protection

8.1.1 Are you transferring personal data to a country or territory outside of the EEA?

Yes No

If no, please go to Part III.

If yes, where?

8.1.2 What are the types of data are transferred? (eg contact details,employee records)

8.1.3 Are sensitive personal data transferred abroad?

Yes No

If yes, please provide details:

8.1.4 What are the main risks involved in the transfer of personal data to countries outside the EEA?

8.1.5 Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?

8.1.6 Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?

8.2 Exempt Transfers

8.2.1 Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply?

Yes No

If yes, what are they?

8.2.2 To which country / territory are these transfers made?

8.2.3 What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle?

Eg consent, (See DPA 1998, Schedule 4, for a full list)

8.3 Choosing a Data Processor

8.3.1 What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?

8.3.2 How did you assess their data security measures?

8.3.3 How do you ensure that the Data Processor complies with these measures?

8.3.4 Is there an on-going procedure for monitoring their data security measures?

Yes No

If yes, please describe. If no, please indicate why not.

III DPP COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

Completed by_____Date_____

Appendix 7

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 Information Governance specialists.

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.

Full scale PIA's will also usually be recommended 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.

Small scale PIA's will normally be required for but not limited to:-

- replacing an existing personal data system by new software.
- design and development of a system where the data held is on consent basis.
- changes to an existing system where additional personal data will be collected.
- proposal to collect personal data from a new source.
- creation or redesign of web-forms for collecting personal data.
- development of new procedures for authentication.

- plans to outsource business processes involving storing and processing personal data.

The screening questions at Appendix 2 should provide a good guide as to which level of PIA, if any, is required.

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

A frequently asked question is whether a PIA can be conducted on a project that is being implemented or has been up and running for some time. 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 Brief/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 including an initial screening process and, depending upon the results, two possible levels of assessment (small scale and full scale) together with a data protection compliance check.

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.