North East Essex
Clinical Commissioning Group

Privacy Impact Assessment Policy

NEECCG POLICY REFERENCE: NEE/CCG/2015/060

Target Audience	Board members, sub-committee members and all staff working for, or on behalf of, the NEE CCG
Brief Description (max 50 words)	Projects that involve using personal information or intrusive technologies give rise to privacy issues and concerns. To enable an organisation to address the privacy concerns and risks a technique referred to a Privacy Impact Assessment (PIA) must be used. Compliance with all North East Essex CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.
Action Required	Once this guidance has been approved, it will be disseminated to all staff and placed on the CCG website/staff Intranet,

Document Information

Title /Version Number/(Date)	Guidance for the Introduction of New Processes (Privacy Impact Assessment)/Version 3.2/Novembe 2016
Document Status *(for information/ action etc.)*and timescale	
Accountable Executive	Chief Finance Officer
Responsible Post holder/Policy Owner	Information Governance Team
Date Approved	7th November 2016
Approved By	Quality Committee
Review Date	March 2019
Equality Impact Assessment	**EQUALITY IMPACT ASSESSMENT** This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to the Board, every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership, and those who work on behalf of the CCG

Brief Summary: Projects that involve using personal information or intrusive technologies give rise to privacy issues and concerns. To enable an organisation to address the privacy concerns and risks a technique referred to a Privacy Impact Assessment (PIA) must be used.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
1.0	25/09/2013	Draft	New document – Privacy Impact Assessment Policy	NHS Central Eastern Commissioning Support Unit, Information Governance Team
1.1	24/10/2013	Draft	Minor amendment made following comments from CCG Quality and Governance Committee	NHS Central Eastern Commissioning Support Unit, Information Governance Team
1.2	07/12/2013	Final	Approved by North East Essex CCG Board	NHS Central Eastern Commissioning Support Unit, Information Governance Team
2.0	22/10/2014	Draft	Changes in ICO guidance and CCG reporting structure necessitates document review. Documents now renamed as 'Guidance for PIA'	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
2.1	28/12/2014	Draft	Amended following comments from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
2.3	28/01/2015	Final	Policy formatted and key contacts amended on page 13.	North East Essex CCG
3.0	22/08/2016	Draft	Amendments and format changes for current year	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.1	26/10/2016	Draft	Personalise and document review	North East Essex CCG
3.2	07/11/2016	Final	Approved by Quality Committee	North East Essex CCG

Contents

1. Introduction

NHS North East Essex Clinical Commissioning Group (the CCG) recognises that the protection of individual's confidentiality and not infringing on their privacy is an essential consideration for the CCG. With the development of new technologies and increased public concerns about intrusion into individuals' privacy, the Information Commissioner's Office (ICO) in conjunction with NHS Digital (formerly the Health and Social Care Information Centre -HSCIC) via the Information Governance Toolkit (IG Toolkit) has identified Privacy Impact Assessment (PIA) as a key tool in addressing confidentiality and privacy concerns.

2. Purpose

Through the PIA process the CCG Information Governance Team (IG Team) will better foresee problems and negotiate solutions to ensure data protection compliance.

Risks that are identified through this process can then be managed through the gathering and sharing of information with key stakeholders (for example Governing Bodies, Audit Committees, patients / service users and staff themselves). Systems can then be designed to avoid unnecessary intrusion into people's privacy where possible and features can be built in from the outset, hence reducing the likelihood of privacy intrusion.

Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that threatens the CCG's credibility and integrity. In order to address this risk, it is advisable that the use of the PIA is seen as a risk management technique.

Carrying out a PIA will increase public confidence in our data collection and the services we provide.

3. Scope

Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives on an individual's privacy. It is important to note that the individuals referred to are patients / service users and staff.

The CCG guidance for carrying out a PIA applies to all individuals involved in the introduction of new processes or proposed changes to existing methods. All relevant staff are required to be familiar with and comply with this guidance.

4. Definitions and terms

Privacy Impact Assessment (PIA)- a process which helps **assess privacy** risks to individuals in the collection, use and disclosure of personal information.

5. Roles and Responsibilities

Accountable Officers for NHS North East Essex CCG

The Chief Officer, as the Accountable Officer, has overall responsibility for information governance within the CCG. The Chief Officer is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner (SIRO) for NHS North East Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Chief Officer. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Quality Committee. This includes oversight of information security incident reporting and response arrangements.

Caldicott Guardian for NHS North East Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing. For the CCG, this is the Director of Nursing and Clinical Quality. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of this.

All Staff

The majority of staff handle information in one form or another. Staff who in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are accountable for ensuring that they are aware of their responsibilities in respect of Information Governance.

Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level, or heads of department responsible for providing assurance to the SIRO that

information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate these.

Information Asset Administrators (IAAs)

IAAs will:

- ensure that guidance in this document is followed;
- recognise actual or potential risks when new processes are being introduced in their directorate / department;
- consult with their IAOs and the CCG IG team to take steps to mitigate risks;
- encourage project / programme leads complete the PIA template at the initiation stage of a project / process.

Managing information risk effectively requires a structured approach involving work areas where accountability sits with senior managers, rather than specialist staff. All staff need to work together to help identify and mitigate information risk.

The Information Governance Team

In order to ensure the investment the CCG makes is proportionate to the risks involved when introducing a new process / service, the IG Team (hosted by Basildon & Brentwood CCG on behalf of Essex CCGs) has developed a PIA template for staff to complete when introducing a process or design (See Appendix 1).

The IG Team should be consulted during the design phase of any new service, process or information asset. The IG team will formally approve IG components including PIAs at the initial stage of the process and this will ensure that the SIRO can provide the necessary assurances to the CCG Quality and Governance Committee and Governing Body.

Where necessary the IG team will seek approval from the Caldicott Guardian regarding the exchange and use of PCD and the need for Information Sharing Agreements

6. Key Principles

Who should carry out a Privacy Impact Assessment PIAs should be completed by key project personnel - this could be the project lead, 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 or upgrades existing systems within the CCG.

Assistance with following this process can be given by the Information Governance Team.

Types of projects or systems that require a Privacy Impact Assessment

The Information Commissioner's Office (ICO) envisages PIAs being used 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'.

PIAs are usually recommended where there is-

- the requirement for a change of the law
- replacement of 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;
- a 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;
- new and intrusive technology to be used; or
- intended reuse of private or sensitive information which was originally collected for a limited purpose in a new and unexpected way.

The core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

PIA terminology often refers to a project as the subject of a PIA and this should be widely construed. A PIA is suitable for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.

- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

What stage a Privacy Impact Assessment can be completed

Unless there is a genuine opportunity to alter the design and implementation of an ongoing project, the ICO recommends that projects which are already up and running are not subject to a PIA process.

The nature of the PIA process means that it is best to complete it at a stage when it cannot 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.

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 (or its equivalent).

Benefits of completing a Privacy Impact Assessment

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 it's objectives, the organisation's requirements and the justifications for particular design features.

- A further benefit of building privacysensitivity 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 CCG 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 ventures 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 1998 already stipulates eight Data Protection Principles, but these only address certain aspects of privacy.

How to 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 lifecycle;
- re-visited in each new project phase;

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

- 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

How to conduct a Privacy Impact Assessment

The following steps should be followed when conducting PIAs:

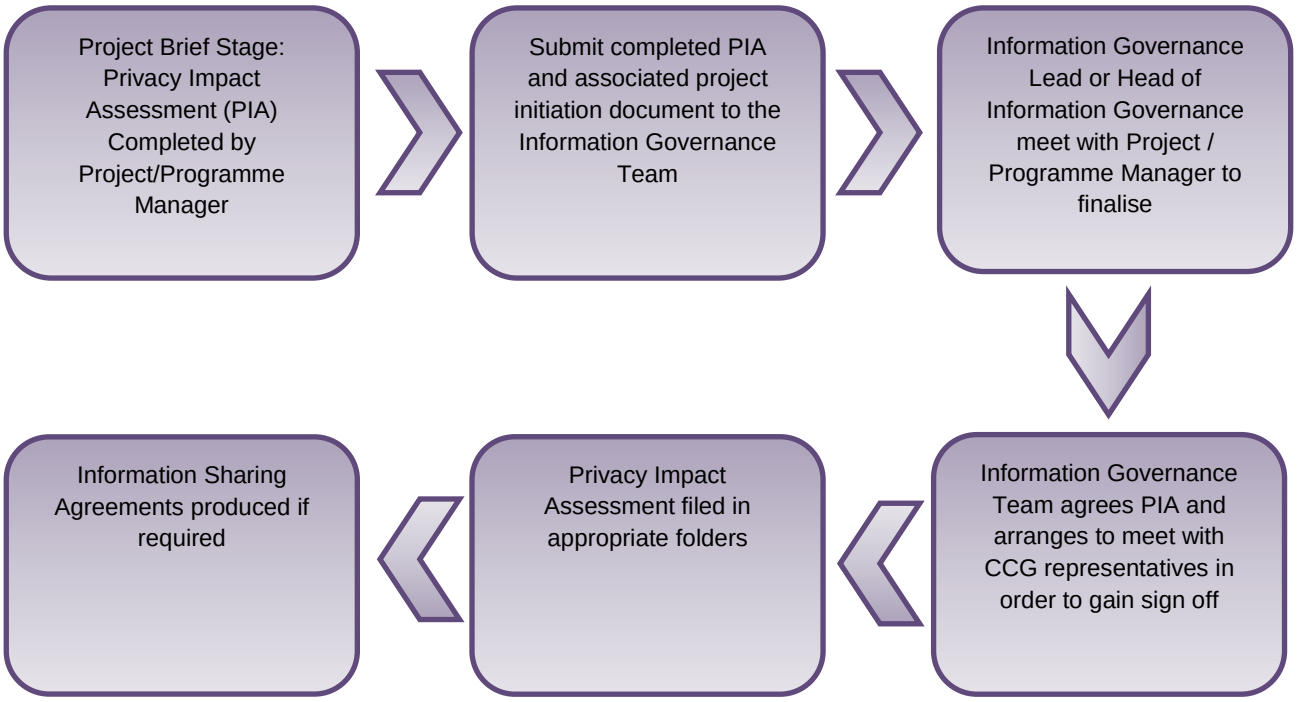
- Project Brief Stage: PIA template completed by Project / Programme Manager
- Submit a completed PIA template and associated project initiation documents to the Information Governance Team via the IG mailbox: essexccgs.ig@nhs.net
- IG Lead or Head of IG meet with Project / Programme Manager to finalise
- IG Team agrees all documentation and arranges to meet with the CCG team in order to gain sign off
- If required, Information Sharing Agreements will be produced
- PIA documentation filed in appropriate CCG folder.

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 outcome

7. Privacy Impact Assessment Approval Process



Completing Privacy Impact Assessment Template

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, albeit sufficient information should be gathered to allow the questions in the PIA template to be applied.

The following three pieces of information are needed when submitting a PIA to the IG team:

- a project outline or a project initiation document;
- Stakeholder analysis;
- an environmental scan;

Please note: Where a Project Lead / Manager is involved this type of information is likely to already be gathered at the Project Brief and Project Initiation Document stage.

Obtain or develop a Project Outline

During the early stages of a project there is only limited documentation available and there may be uncertainty about the scope and features of the intended system.

A copy of the project initiation documents, such as a project charter or terms of reference should be obtained at the beginning so that it is clear what the potential impact of the project might be.

If such documents are not available, consult with relevant staff in the organisation, 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.

Where the activity is conducted at a later stage of the project, much more information will be available and the project outline should provide references to relevant documents, including descriptions of relevant technologies, predecessor systems and / or similar projects elsewhere.

Stakeholder Analysis

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

- 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 a broad list of groups with a very brief description of the stake each group might have in the project should be compiled.

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.

Environmental Scan - Seeing what else is out there

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 organisation, or 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. Possibilities include DH and NHS England but the orientation and expertise of organisations like these may vary over time.

- 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 one to two page summary with reference to working documents generated during the process should be enough.

8. Completing Privacy Impact Assessment Template

Once the preparation has been concluded and the information collated the PIA template should then be completed. This involves answering the questions set out in Appendix 1.

The purpose of the PIA template is to ensure that the investment the organisation 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.

The requirement to address and identify whether or not a PIA is required for any project forms part of the project process. The IG team will act as monitors to ensure that documentation is completed at the appropriate stage. The IG Lead and Project / Program Managers will re-evaluate the PIA process throughout the project development and implementation process.

9. Audit and Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events

- Reporting IG work programs and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external assessments or other sources of information and advice.

10. Dissemination and Implementation

The policy will be published on the intranet and staff shared drive. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels e.g. through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

This document will be subject to review when any of the following occur:

- Where the adoption of the standards highlights errors and omissions in its content
- Where other standards / guidance issued by the CCG conflict with the information contained.
- Where good practice evolves to the extent that revision would bring about improvement.
- 2 year elapse after approval of the current version.

11. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

12. Related Documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Information Governance Policy
- Data Protection & Confidentiality Policy

13. Equality & Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

14. Key Contacts within the CCG Within the CCG

Senior Information Risk Owner	Chief Officer – Sam Hepplewhite
Caldicott Guardian	Director of Nursing and Clinical Quality – Lisa Llewelyn
CCG IG Champion	Business Systems and Development Manager – Laura Ellis

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net

Appendix 1 - Privacy Impact Assessment Procedure.

For Use With:

- New projects
- Changes to existing projects/procedures/systems
- Information Sharing Protocols
- Relocation of staff or equipment

Please complete this document in conjunction with the Privacy Impact Assessment Guidance Document

Does this project require a Privacy Impact Assessment?

Does the project include the use of personal confidential or commercially sensitive information? If the answer to this question is yes then this document must be completed.

Information Governance
Privacy Impact Assessment Template

Projects that involve processing or sharing personal information or intrusive technologies give rise to privacy issues and concerns. To enable an organisation to address the privacy concerns a privacy impact assessment (PIA) can be used to assess privacy risks to individuals in the collection, use, disclosure and disposal of information. The PIA can help identify privacy risks, foresee problems and bring forward solutions.

Project Information	
Project Name:	Date:

Organisation: Sponsor (for example Project Board)	
Background: Why is the new system / change in system / sharing of information required?	
Benefits:	
Constraints:	
Does the project involve multiple organisations? If yes – name them, and their project lead details:	

Work package details

Project		Point of contact for this work (name, role, phone, e-mail)	
		Specific area concerned	
Project summary			

Brief description of overall activity			
Has anything similar been undertaken before			
Is there a reason why an Impact Assessment is not required for this piece of work			
Stakeholder(s) / Organisation(s) involved			
Sponsor (for example Project Board)		Activity period	

Information

What information will be collected – be specific (Person Identifiable Data (PID), Corporate, Sensitive and so on.)	
Why is information being collected	
How information is being collected	Verbal and Other ☐→
How information is to be stored	Paper ☐ Electronic ☐ Other ☐→

Where information will be stored (including back ups and copies)	
How information is to be edited or deleted	
How data is to be quality checked	
Who is responsible for the information	
What are the benefits to the individual and professional	
As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the questionnaire below	
	 Cloud Screening Questions.docx

Sharing and access

What information is shared	
Who are you sharing with	
How information is to be transported	
Which roles will have access. Is there any restrictions based on different roles	

How is it accessed	
How access is to be monitored (audit, logs)	
What security measures will be in place	
What information sharing protocols and operational agreements will be in place	
What training is planned to support this piece of work	
What is the process for obtaining and recording consent / dissent (how, where, when, by whom)	
If consent has not been obtained, is there a legitimate reason to share?	
Will reports be generated from this information. If yes, will this be identifiable or anonymous (will the reports be used for research)	
How can the individual access the information	

Retention

How long data is to be retained	
What is the process for start-up and closing down this piece of work	

If the organisation / service ceases what will happen to the information	

Risks, issues and activities

Any known risks or issues	
Any known activities that will have a direct effect on this piece of work	

Outcome of Information Governance Team PIA Panel

Signed on behalf of the Information Governance Team, [Enter organisation name]

Name: [Enter Name], Head of Information Governance (or equivalent)

Signature: ……. Date: ……..

Signed on behalf of [Enter organisation name]

Name: ……..... SIRO / Caldicott Guardian

Signature: …… Date: ……