PRIVACY IMPACT ASSESSMENT (PIA) PROCESS

1. Purpose of this document

The Care Quality Commission (CQC) has a legal and ethical duty to protect, and to avoid unnecessary interference with, the privacy of individual people.

In order to carry out our functions, we are required to undertake actions that may impact upon the privacy of:

- people who use the services we regulate, their families and carers
- providers and managers of these services, and their staff
- our own staff, and the staff of other organisations we work with
- other members of the public

It is vital that the likely impact of CQC's actions upon the privacy of these people is understood and that the risks to privacy are robustly managed. Any interference with personal privacy must be minimised as far as possible, and must be appropriate and proportionate.

This document establishes a defined Privacy Impact Assessment (PIA) process, to ensure that we have a consistent and adequate means to achieve this.

The PIA process set out in this document is based upon the *Privacy Impact Assessment Handbook; version 2.0*, published by the Information Commissioner's Office (www.ico.gov.uk) and is tailored to the needs of CQC.

2. What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is an exercise to assess and understand the potential impact that planned actions of CQC may have upon the privacy of individuals, and to develop solutions to manage risks to privacy and minimise the potential impact upon privacy.

A PIA may, or may not, include external consultation. It may be conducted as a stand-alone piece of work or may form part of a wider piece of work - such as a formal public consultation process (under the *Code of Practice on Public Consultations*) or the piloting of a new process.

3. Why do a Privacy Impact Assessment (PIA)?

The main purpose of undertaking a PIA is to ensure that risks to the privacy of individuals, arising from the actions of CQC, are identified and robustly managed so as to avoid unnecessary impact upon the individual privacy, dignity and well-being of people whose personal information we process.

Performing a PIA at an early stage of planning any proposed change avoids problems being discovered at a later stage, when the costs of making significant changes will be much greater.

The PIA process allows privacy solutions to be considered and implemented at an early stage, and as a fundamental part of key processes – rather than a later 'add-on' – so facilitating the development of processes which allow more robust and confident processing of personal information.

The PIA process also helps provide assurance that CQC will meet all of its legal and government requirements in relation to processing personal information and protecting privacy.

By addressing privacy issues in a transparent and structured manner, the PIA process will increase trust in CQC and protect the reputation of the organisation.

These outcomes will support the strategic aims of CQC by allowing us to make more effective use of information to achieve the greatest impact, strengthening joint working with strategic partners (where that work involves sharing or joint use of personal information), and continuing to build better relationships with the public and organisations providing care.

3. Key definitions

Privacy is a fundamental issue of the integrity of an individual; their ability to choose and control what aspects of their person, their information and their behaviour are known to others, and to the protection of this choice and control from unsanctioned intrusion.

For the purpose of CQC's PIA process, the interpretation of 'privacy' can best be defined in relation to the privacy of personal information, and the privacy of the person.

> **Privacy of personal information** is the quality of privacy in relation to recorded information that identifies, or could potentially identify, individuals. Changes to the personal information we collect, record, analyse, use, share, disclose or dispose of, or to the protections that we place upon these processes, may have an impact upon the privacy of personal information. In most cases, the privacy of personal information will be the main issue of consideration within CQC's PIA processes;
>
> **Privacy of the person** is the quality of privacy in relation to the body, actions or behaviour of a person. Any process introduced by CQC which relates to observing care, surveillance of individuals, or the monitoring of communications will impact upon the privacy of the person.

Projects, for the purpose of this document, is the term used to describe any planned process by which CQC changes the ways in which it does things. This includes formal programmes or projects being carried out using CQC's defined methodology, but also includes the development of new policies, processes, methodology, guidance or training.

Project lead is the person with overall responsibility for delivery of a 'project'. This person may delegate responsibility for aspects of that project, including the PIA process, but retains responsibility for delivery. Wherever this document refers to the 'project lead' it should be read as the person with overall responsibility *or* the person who has been delegated by that person with regard to performing the task in question.

Personal information is information that relates to, and identifies, an individual – either on its own, or when combined with other information held by CQC or likely to be available to any recipient of information provided by CQC. **Personal data** has a specific meaning within the Data Protection Act 1998. Any personal information relating to living individuals that is processed by CQC is likely to be personal data as defined by that Act.

Processing means obtaining, recording or holding information, or carrying out any operation on the data, including; organisation, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, publication, alignment, combination, blocking, erasure or destruction. In effect, anything that CQC does with information or data should be considered to be 'processing'.

4. Objectives of the PIA?

The key outcomes that a PIA should seek to achieve are:

- the identification of the project's potential privacy impacts and risks;
- 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;
- management of information risk, and other risks to privacy, by:
    - 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 of the outcomes.

5. Managing a PIA

The responsibility for conducting a PIA is placed upon the project lead.

Depending upon the nature and type of the project, and the resources available, the task of conducting the PIA may be delegated, outsourced to an external organisation and/or overseen by a project team.

Any person delegated to undertake a PIA must be in a position to influence the design and development of the project, and to participate fully in the project design decisions.

The Information Rights Manager, Information Security Manager and the Information Governance Group will provide advice to the project lead, as required.

The Information Rights Manager is responsible for maintaining a PIA log, and will retain copies of all PIA 'initial screening assessments' and 'PIA reports'.

The Senior Information Risk Owner (SIRO) is responsible for reviewing PIA initial screening assessments, assessing the requirement to conduct a PIA, and signing off PIA Reports. The SIRO will be supported by the Information Rights Manager and Information Governance Group in performing this role.

In the absence of the SIRO, their responsibilities in relation to PIAs may be performed by CQC's Information Governance Group (IGG), with collective decisions made by consensus and signed-off by the Deputy Chair of that group.

The Chair of any committee of CQC which approves projects (including changes to policy, methodology or guidance) is responsible for ensuring that the PIA process has been followed, by checking that the project has either:

- No reasonably foreseeable impact upon privacy (i.e. does not involve any significant change to the way in which personal information is processed); or that the Project Lead has undertaken
- An initial screening assessment, with a decision from IGG that a full or small scale PIA is not required; or
- A PIA Report, which has been reviewed and assessed by IGG as adequate to comply with the requirements of this process.

6. Managing privacy risk

Any privacy risk or information risk identified during the PIA process (including initial assessment) must be managed in accordance with CQC's Risk Management policy and processes.

7. Privacy Impact Assessment (PIA) process

Initial preparation

Some work is required before an initial PIA assessment can be undertaken for any project:

- The purpose and objectives of the project must be sufficiently defined in order to be able to meaningfully articulate the proposed change to CQC's way of working,
- An initial consideration must be made as to whether the proposed change is likely to have an impact upon personal privacy, for example by;

    - Introducing new processes for observing, monitoring or tracking the movements or actions of individuals,
    - Changing the way in which we collect, obtain or record personal information,
    - Combining items of personal information in a new way,
    - Combining items of anonymised (or pseudonymised) information in such a way as raises the risk that individuals may become identifiable,
    - Changing the way in which we store, analyse, manage, or dispose of personal information,
    - Reducing the level of protection provided to personal information,
    - Disclosing, sharing or publishing personal information in a new way,
    - Disclosing, sharing or publishing anonymised (or pseudonymised) information in such a way as raises the risk that individuals may become identifiable when that information is combined with information available to potential recipients of the information,
    - Introducing new technologies or information systems for collecting or processing personal information.
- It is recommended that you should consider whether there is any available evidence of privacy impact for similar projects in the past – either relating to previous actions of CQC or other, comparable organisations,
- It may be appropriate to conduct initial consultations with relevant stakeholders, so as to begin to understand the likely impact and acceptance of the proposed change,
- You should review CQC's *Code of Practice on Confidential Personal Information* and *Information Security Policy* and seek advice from the Information Rights Manager (where there are any questions as to compliance with the Data Protection Act 1998, or other laws relating to personal information) and/or the Information Security Manager (where there are changes which relate to the security of information).

Initial assessment

Once you have undertaken the initial preparation, you should perform an initial assessment and report the outcome of that assessment using CQC's Equality and Human Rights Duties Impact Analysis form (Appendix A).

If you require any assistance or advice in completing the form, you should contact the Information Rights Manager.

The form gives a space to provide a summary of any consideration of privacy issues that have already been undertaken. This would include any relevant work undertaken at the preparation stage, such as consideration of previous, similar projects, or initial consultation or discussion with stakeholders. Steps that have already been put in place to protect privacy can also be described here. Supporting documents may be attached, if necessary. The SIRO will give careful consideration to this information when deciding whether a further stage of PIA is required.

Completing the form requires you to undertake an initial assessment of risks *relating to potential impact upon the privacy of individuals* and to set out the actions that will be taken to avoid, mitigate or manage those risks.

Each action must have an owner assigned to it. This person must be aware that they are being assigned the action and must have accepted it.

Once completed, the project lead must submit the form to the Information Rights Manager. The Information Rights Manager will review the form and make a recommendation to the SIRO. The SIRO will reach one of the following decisions:

- No further assessment required
- Full scale PIA required
- Small scale PIA required
- Further information needed to complete assessment

The SIRO will also assess whether any of the following are required:

- Legal compliance check
- Security Exception Risk Acceptance (SERA)
- Caldicott approval

All initial assessments, and SIRO decisions, will be reported to CQC's Information Governance Group.

When will the SIRO require a further PIA to be conducted after initial screening?

Following review of the initial screening assessment, the SIRO will require that a full or small scale PIA be conducted in circumstances where they are not sufficiently assured that the privacy implications of a project are already fully understood by CQC, or where they consider that the potential privacy implications of the project are so significant that further consultation on them is necessary in order to maintain public trust in CQC.

The SIRO will be mindful of the resource implications of performing a full PIA, and will only require such an exercise for the projects where there is the greatest potential for impact upon privacy. By and large, these are likely to be significant programmes of work, or large projects, involving major changes to the way in which CQC works.

Any PIA required by the SIRO is the *minimum* requirement for the project. The project lead may choose to conduct an assessment which goes above and beyond this requirement.

The SIRO may require that more than one PIA is required for a project, for example requiring the PIA to be conducted at appropriate stages or checkpoints in a large project.

Guidance on conducting a full scale PIA is in Appendix B

Guidance on conducting a small scale PIA is in Appendix C

Legal compliance check

Where the SIRO considers that the project has implications in relation to compliance with legal requirements which relate to confidentiality, privacy or data protection, they will require that the project should be subjected to a legal compliance check. This may be in addition to the requirement to undertake a PIA.

The legal compliance check is a requirement that the Information Rights Manager (or another person, chosen by the SIRO) must be consulted on the project (on an ongoing basis, where necessary) so as to provide guidance on ensuring compliance with relevant legal requirements (for example the Data Protection Act 1998, the Human Rights Act 2000, and the provisions relating to confidential personal information within the Health and Social Care Act 2008).

Where further advice is required from CQC's Legal Services team, or in the form of external advice, this will be arranged by the Information Rights Manager.

Security Exception Risk Acceptance (SERA)

Where a project will involve deviation from CQC's current Information Security Policy or information system security measures, a Security Exception Risk Acceptance (SERA) must be completed and submitted so that any information risk arising from this deviation can be assessed and approved by the Senior Information Risk Owner (SIRO).

Full guidance on the SERA process is available **[link]**

Caldicott approval

Where a project will involve a significant change in, or deviation from, the way in which CQC processes identifiable information about people who use the services we regulate, this proposal must be approved by CQC's Caldicott Guardian.

The Caldicott Guardian's role is to consider whether the proposed processing of service user information complies with the 'Caldicott Principles', which are:

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary.

Personally identifiable information items should not be used unless there is no alternative.

Principle 3: Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4: Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

Principle 5: Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Principle 6: Understand and comply with the law.

Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

An application form for Caldicott Approval will be provided by the Information Rights Manager.

Ongoing review

It is the responsibility of the Project Lead to identify changes or developments in a project (or wider issues impacting upon the project) which are likely to significantly change the privacy risk and potential privacy impact. In such cases, advice should be obtained from the Information Rights Manager and it may be necessary to initiate a new PIA process by completing a new Initial Assessment Form for consideration by the Information Governance Group.

Risks and issues identified during the PIA process must be managed under CQC's Risk Management Processes, and must remain upon relevant risk registers until they can be removed in accordance with that process.

Records of the PIA must be retained by the Project Lead and may be audited.

Privacy protections and other risk mitigations may be subject to Internal Audit.

APPENDIX A

Care Quality Commission: Equality and human rights duties impact analysis (decision making and policies)

Equality Act 2010
Human Rights Act 1998

For advice on completion from the Involvement and EDHR team, please use the Ask regulatory development mailbox: askregulatorydevelopment@cqc.org.uk

1.

Identifying Name (name of project, policy, work, or decision)	
Intended outcomes (include outline of objectives or aims)	
Who will be affected? (People who use services, CQC staff, the wider community)	

2.

For the record	
Who carried out the analysis	
Current Version number	
Date analysis completed:	
Name of responsible Director/Head	
Date analysis was signed off by Director/Head:	
Involvement & EDHR sign-off name	
Date of EDHR sign-off	

3.

• Does the work affect people who use services, employees or the wider community? (This is not only refers to the number of those affected but also by the significance of the impact on them)	Yes/No
• Is it a major piece of work, significantly affecting how functions are delivered?	Yes/No
• Will it have a significant effect on how other organisations deliver their functions in terms of equality or human rights?	Yes/No
• Does it relate to functions that previous engagement has identified as being important to particular protected groups or human rights?	Yes/No
• Does or could it affect different protected groups differently?	Yes/No

• Does it relate to an area with known inequalities or breaches of human rights?	Yes/No
• Does it relate to an area where equality objectives have been set by CQC?	Yes/No
• Does or could it impact upon personal privacy? For example by: • Using personal data (information about identifiable individuals) in new or significantly changed ways, or for new purposes. • Collecting new identifiers (i.e. information which identifies people, such as name, D.O.B., NHS number, postcode etc). • Combining anonymised data sources in such a way as to risk identifying individuals? • Disclosure or publication of personal data or identifiers. • New or additional information technologies with substantial potential for privacy intrusion (e.g. surveillance, image or video recording of individuals, tracking or monitoring of individual). • Observing or monitoring with potential for privacy intrusion (e.g. observing intimate personal care).	Yes/No

If the work does or could impact upon personal privacy, explain how (for example: what additional information is being collected, used or shared?) If there is no anticipated impact upon personal privacy, skip this box and continue below.

4.

Do the answers above indicate that this work is relevant to equality or human rights? If yes skip this box and continue below. If no, document the reasons below and forward this EHRDIA to Involvement & EDHR team for sign-off
(Include details of evidence analysed to support this decision)

5.

Engagement and involvement • Have you involved people who use services, staff and other stakeholders? • What are the key findings of your engagement relating to equality and human rights? Include known representation across the characteristics protected in the Equality Act: age, disability, gender, gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion and belief, and sexual orientation.	
Target Group	**Summary of Involvement**
People who use services	
Staff	
Other stakeholders	

6.

Evidence List the main sources of data, research and other sources of evidence reviewed to determine impact on each protected characteristic, human rights or privacy. If there are gaps in evidence, state what you will do to close them in the Log of Equality & Human Rights Actions	
Age: (include younger as well as older people, safeguarding, consent and child welfare)	
Carers: (impact of part-time working, shift-patterns, general caring responsibilities)	
Disability: (include attitudinal, physical and social barriers)	
Gender: (men and women)	
Gender Reassignment: (transgender and transsexual people, issues such as privacy of data and harassment):	
Pregnancy and maternity: (impact of working arrangements, part-time working, infant caring responsibilities and breastfeeding)	
Race: (include differences between ethnic groups, nationalities, gypsies and travellers, language barriers)	
Religion or belief: (include different religions, beliefs and no belief)	
Sexual Orientation: (include impact on heterosexual people as well as lesbian, gay and bisexual people)	
Human Rights (refer to Guidance for examples, includes privacy)	

7.

Analysis Considering the evidence and engagement activity, set out below the actual or likely effect of the policy, project or work under each of the general duties of the Equality Act. CQC must have due regard to the general duties in the exercise of all of its functions	
Effect on eliminating discrimination, harassment and victimisation (includes unlawful discrimination because of marriage or civil partnership status, as well as other protected characteristics)	
Effect on advancing equality of opportunity (includes removing or minimising disadvantages, taking steps to meet the needs, and encouraging participation in public life of people from protected groups)	
Effect on promoting good relations between protected groups	
Effect on compliance with Human Rights Act 1998	
Privacy impact (Includes assessment of risks to personal privacy. Privacy issues will be reviewed by the Information Governance Group who may require further privacy impact assessment work)	

8. Log of Equality and Human Rights actions

Give an outline of the key actions based on any information gaps, risks, challenges and opportunities identified during engagement and evidence analysis. Include any action required to address specific equality, human rights or privacy issues where the work may need adjusting to remove barriers or better advance equality as well as actions to mitigate any potential negative effects of the policy on particular groups . Include how the actual impact on equality and human rights will be reviewed after implementation of the policy or project. Add more rows if required. Refer to Guidance for more information

Action (If using a project plan this should be a new deliverable or new task within an existing deliverable)	**Start date**	**End date**	**Action Owner**	**Outcome** (relate back to analysis section – which equality or human rights issues will be addressed through this action)	**Success measure**	**Actual Completion Date**
Monitoring equality and human rights in operation: (add method or remove)						
Reviewing equality and human rights in operation: (add method or remove)						

Guidance:
How to complete Equality and human rights duties impact analysis (decision making and policies) - EHRDIA

The purpose of an EHRDIA is to ensure that the Care Quality Commission integrates consideration of equality and human rights into its day to day business. The Equality Act 2010 requires organisations to consider how they could positively contribute to the advancement of equality and good relations in everything they do. The Human Rights Act 1998 also requires us to be compliant with the Act in the way we carry out our work.

EHRDIAs are not just about identifying discrimination but also about identifying opportunities for promoting equality, and promoting good relations for people with protected characteristics. Details of positive impacts help to demonstrate how the piece of work contributes to equality and inclusion, especially for groups protected by equality legislation.

It is not sufficient to say that the policy is intended to benefit everyone and will advance equality across all the groups. An effective equality analysis will help ensure that particular needs are taken into account, whether there are varying degrees of benefit, and any wider effects of the policy.

This is not a tick-box exercise. This EHRDIA should be used to document how equality, diversity and human rights have been considered in every part of the process. Even the decision as to whether an EHRDIA is required, requires the exercise of judgement. This in turn highlights the necessity for involvement and engagement of those people who will or may be affected.

Engagement and involvement
CQC is committed to involving people who use services in our work. We are also required by legislation to engage with people who have an interest in our equality performance. Involvement should start from the very beginning and before important decisions have been made.

Evidence
The Equality Act 2010 requires CQC to consider not only information it already holds, both qualitative and quantitative, but also to identify any information gaps, and take steps to fill those gaps. Local, regional and national research can be used. Evidence includes information learnt during engagement and involvement.

Case law has established that CQC should keep an accurate, dated, written record of the steps taken to analyse the impact on equality.

Human Rights
Most human rights can be captured under the headings of FREDA: fairness, respect, equality, dignity and autonomy, except for Article 2: the right to life. However the equality element of human rights is best analysed separately, looking at the impact on each protected characteristic under the Equality Act.

The Human Rights Act includes the right to privacy. CQC must only interfere with this right where it is proportionate and in the public interest to do so for the purpose of protecting health or public safety, or for the prevention of crime, or for the protection of the rights and freedoms of others. It is therefore necessary to assess the potential impact of any proposed change upon the privacy of individuals.

Log of Equality and Human Rights Actions

In addition to any other items that might be appropriate, the log should be used to record and monitor:

- any steps needed to reduce information gaps
- any changes to the policy or project required that relate to equality and human rights as a result of engagement and involvement, or analysis of evidence. This includes changes to :
    - remove barriers to equality
    - advance equality or human rights
    - mitigate any potential negative effects on a particular group.
    - It is lawful under the Equality Act to treat people differently in some circumstances, for example taking positive action or putting in place single-sex provision where there is a need for it.
    - It is both lawful and a requirement of the general equality duty to consider if there is a need to treat disabled people differently, including more favourable treatment where necessary.
    - The policy must be stopped or removed if the EHRDIA indicates that it will result in unlawful discrimination. Removal should also be considered if it will result in adverse effects on equality that cannot be justified or mitigated.
- How you will review the actual impact of the policy or project on equality and human rights after implementation
- This log should be monitored as part of the overall project plan monitoring.
- Where a formal project plan is being used, it is recommended that actions in the log are added to the deliverables or tasks in the overall project plan – so that they are integrated into the project work

Privacy impact assessments

Where a proposal has a potential impact upon personal privacy, the analysis will be reviewed by the CQC Information Rights Manager, and must be signed off by the Senior Information Risk Owner (SIRO).

Where the SIRO consider that the potential privacy impact may not be fully understood, or where privacy risks may be particularly significant, they may require you to undertake a further privacy impact assessment (PIA) in accordance with the Privacy Impact Assessment Process [link]. This will usually be required for very significant change programmes with privacy implications, but may be required for proposals of any type or size.

The process allows for scalability of the PIA, commensurate with the size of the programme or project.

For most proposals, a further PIA will not be required, providing that this issue has been given reasonable consideration as part of the EHRDIA. You should read the PIA process/guidance before completing relevant sections of the form..

Publication
Each EHRDIA should be published on the internet, intranet and/or together with the main publication document whatever is most appropriate. You may wish to remove your name and contact details prior to publication.

Governance
All EHRDIAs must be authorised by a Director of Business or Head of Function. Each completed EHRDIA must be signed-off by a member of the Involvement and EDHR team prior to publication.

To contact the Involvement and EDHR team, please use the Ask regulatory development mailbox

After implementation
We are required to demonstrate the impact of our policies and methodology on employees, people who use services and others from protected groups. Consider the timescale of the implementation and delivery when deciding on monitoring and review dates. The monitoring activities should form part of the Action Plan and relate to the success measures and outcomes.

Further information about statutory duties

- Equality and human rights on our intranet
- Guidance on the public sector equality duty from the Equality and Human rights commission

APPENDIX B

Full scale PIA

A full scale PIA is a detailed and robust review of the privacy implications of a project, carried out over five phases. Full scale PIA will only be required for the most significant projects with the greatest potential for impact upon personal privacy – for example, a substantial change in the way in which CQC collects and uses service user information during inspection. In most cases, these projects will already include a consultation phase, and the PIA can be incorporated within this overall consultation, if desired.

More detailed information about conducting full scale PIA's can be found in the Privacy Impact Assessment Handbook, produced by the Information Commissioner's Office. This section of this document is drawn from the PIA Handbook, and tailored to the needs of CQC

Phase 1: Preliminary phase (full scale)

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 for the PIA.

The following tasks are recommended:

- Identify a lead, and assign the task of carrying out the PIA.
- Establish a project team, with terms of reference, to oversee the PIA, if appropriate. It is recommended that the Information Rights Manager should be invited to join the PIA project team.
- Ensure at this stage that the project terms of reference, the scope, and the resources dedicated are adequate and appropriate to conduct the PIA.
- Review the outcomes and any documents from the initial privacy assessment. If necessary, prepare any documents that were not produced during the initial assessment and which might be helpful in completing the PIA.
- Identify and hold preliminary discussions with internal stakeholders and relevant organisations. These discussions would generally focus on relevant parts of the organisation itself and any key participating organisations.
- Identify and 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 initial screening process.

These tasks are suggested to assist you in preparing the project background paper. This document will establish the basis for discussions with stakeholders.

The project background paper should contain, or should be developed to include, the following:

- 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 organisation'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 at the time the document is prepared.
- Brief descriptions of options and sub-options that have been 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.

Phase 2: Preparation phase (full scale)

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 (PIACG).

The following tasks are recommended:

- Develop a consultation plan to ensure that discussions with stakeholders are effective.
- Form a PIA consultative group (PIACG). This comprises representatives of stakeholder groups.
- Distribute the project background paper to the PIACG. This ensures that the PIACG 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 you make the most of the consultation and analysis phase, it is useful to put a consultation plan in place.

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 provide information 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 PIACG members evaluative comments that avoid exposing the information).

<u>Phase 3: Consultation and analysis phase(s) (full scale)</u>

This 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 recommended:

- 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'. The issues register 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 PIACG; and
    - the project team.
- Pass the project team's feedback to the PIACG.
- Conduct further consultations with the PIACG.
- Incorporate the decisions on privacy design features into the project 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 (eg 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.

Phase 4: Documentation phase (full scale)

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 recommended:

- 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 PIACG.

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.

The following are key elements of a PIA report for a full-scale PIA:

- 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.

Phase 5: Review and audit phase (full scale)

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 recommended:

- 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 PIACG.
- Present the privacy review report to the Information Governance Group
- Ensure that any risks and mitigations are reflected in the appropriate project and corporate risk registers.
- Make the privacy review report publicly available, if appropriate.

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.

The Senior Information Risk Owner (SIRO) will sign off the PIA Report, or stipulate any further actions required to adequately complete the PIA.

The SIRO may recommend that review of any privacy safeguards and information risk management/mitigations may be incorporated into CQC's internal audit processes.

APPENDIX C

Small scale PIA

Due to the time and resource implications of conducting a full scale PIA, CQC will only conduct such assessments in exceptional circumstances – usually for the largest and most high-risk projects.

In most cases, where a PIA is required following initial screening, a smaller scale and less formalised PIA will be conducted.

Small scale PIAs should follow the same five phase process, but require less exhaustive planning, information gathering, analysis and documentation.

Phase 1: Preliminary phase (small scale)

The purpose of this stage is to develop an overall plan for how the PIA will be conducted, and to begin to develop the background material for consultation.

To achieve this, the following tasks are recommended:

- Identify a lead, and assign the task of carrying out the PIA.
- Identify relevant stakeholders that should be consulted as part of the PIA, this may include; internal stakeholders (other CQC staff), strategic partners, registered persons and bodies, people who use services and their representatives.
- Review the initial assessment, and any feedback from the Information Governance Group, and establish the key privacy issues that require consideration.
- Prepare a background paper, to be used in the consultation.

The purpose of the background paper is to provide consultees with the information required to understand the proposals, so as to facilitate their feedback. It should contain:

- A statement of the project's objectives, scope and rationale (i.e. what we are planning to do and why).
- An explanation of how this differs from what currently happens.
- A description of how it is proposed to implement the change in practice.
- An initial assessment of the key privacy issues and risks.
- A brief description of any options that have been identified, including both those that have already been dismissed (and why) and those that remain under consideration.
- Any other information or supporting documents required to understand the proposals.

It is recommended that the background paper should be reviewed by the Communications Delivery team, especially where public consultation is planned. This will help to ensure that the document is clear and easy to understand.

Phase 2: Preparation phase (small scale)

The purpose of this phase is to make the arrangements needed to enable the consultation and analysis to run smoothly.

To achieve this, the following tasks are recommended:

- Decide how various stakeholders will be consulted. It may be adequate and appropriate to consult with standing stakeholder groups (of providers and service users), but in some cases a wider consultation may be required or the consultation will form part of a pilot exercise.
- Decide how consultees will feed back to CQC (e.g. by answering a questionnaire, or through workshops) and make appropriate plans for these.
- Prepare a consultation plan, and send it to the Information Rights Manager.

The consultation plan will be a short document setting out who will be consulted on the proposals, and how this will be done. The background document (prepared as part of phase 1) and any other relevant documents (such as questionnaires or workshop presentations) should be provided.

The consultation plan will be reviewed and must be approved by the Information Rights Manager.

Phase 3: Consultation and analysis phase (small scale)

This phase involves the actual consultation with stakeholders, and the collection and analysis of feedback.

This consultation may be a stand-alone process, or part of a pilot exercise or broader consultation process (i.e. a consultation that looks at other issues in addition to privacy).

Feedback on privacy issues should be collected and reviewed so as to identify any additional privacy risks or issues that had not previously been identified *and* to review and re-assess the existing privacy risks and issues.

Phase 4: Documentation phase (small scale)

This phase involves the preparation of a Privacy Impact Assessment report.

The following are key elements of the PIA report:

- A description of the project
- A description of the consultation process, including a list of organisations and groups consulted. Where individuals have provided responses, you should say how many and who they were (e.g. 7 service users and 2 family members) but should not identify individuals.
- An analysis of privacy concerns, issues and risks raised.
- An updated risk assessment (updated from the risk assessment in the initial screening assessment).
- Discussion of the alternatives considered, the decision made, and the rationale for this decision (i.e. what changes are we going to make and why?)
- A description of any privacy design features or information risk mitigations being implemented to reduce or avoid privacy intrusion.
- An analysis of the public and stakeholder acceptability of the proposals (i.e. how controversial and/or unpopular is the proposed change likely to be).

Phase 5: Review and audit phase (small scale)

The PIA report must be submitted to the Information Rights Manager.

Any risks and mitigations must be transferred into the appropriate project and corporate risk registers.

The Senior Information Risk Owner (SIRO) may recommend that review of any privacy safeguards and information risk management/mitigations may be incorporated into CQC's internal audit processes.

The SIRO will sign off the PIA Report, or stipulate any further actions required to adequately complete the PIA.

For some projects, several PIAs may be conducted during the project lifecycle.