NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Data Protection Impact Assessment Policy and Procedure

Ratification Process

Lead Authors:	Corporate Services Manager (IG Lead/DPO) Corporate Services Support Manager (IG)
Developed by:	Information Governance, Business Intelligence and IM&T Steering Group
Approved by:	Information Governance, Business Intelligence and IM&T Steering Group
Ratified by:	Integrated Performance and Assurance Committee
Date ratified:	28 May 2019
Version:	1.0
Latest Review date:	May 2021 (or earlier if needed in the light of new legislation or guidance)
Valid on:	28 May 2019

DOCUMENT CONTROL SHEET

Development and Consultation:	Policy developed in accordance with new guidance under the Data Protection Act 2018. Document approved by the CCG's IG, BI and IM&T Steering Group and endorsed by the Integrated Performance and Assurance Committee (IPAC).
Dissemination	This policy will be promoted within the CCG and uploaded to the staff DPIA extranet page and the public website.
Implementation	The CCG's Senior Information Risk Owner (SIRO) is responsible for monitoring the application of the policy by ensuring that: The Policy is brought to the attention of all employees; Managers are aware of their responsibilities for ensuring that staff under their control implement the Policy; Appropriate training and guidance is provided to staff; Corporate business processes support the implementation of this Policy.
Training	Training will be undertaken if required as part of the CCG's ongoing processes.
Monitoring	• CCG Senior Information Risk Owner (SIRO) • CCG Data Protection Officer (DPO) / IG Lead • CCG Senior ICT Service Development Manager • IG, BI and IM&T Steering Group
Review	The Information Governance Team is responsible for reviewing this Policy. Review will take place two yearly, or earlier if there are changes in procedures or legislation.
Links with other documents	The policy should be read in conjunction with: • Code of Conduct for Employees in Respect of Confidentiality; • Data Protection Policy; • Information Governance Policy and Management Framework; • Records Management and Lifecycle Policy; • Data Quality Policy. • DPIA Staff Extranet Page
Equality and Diversity	The IG Administrator has carried out an Equality & Diversity Impact Assessment and concluded that the Policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

REVISIONS

Version	Page/Section number	Description of Change	Date Approved
1.0	Whole document	New Policy and Procedure document translated from the CCG's DPIA Process Guidance.	May 2019

TABLE OF CONTENTS

1 PURPOSE

The General Data Protection Regulation (GDPR) May 2018 introduced a new obligation upon organisations to conduct a Data Protection Impact Assessment (DPIA) before carrying out types of processing (See Appendix 1) likely to result in high risk to individuals' interests.

Projects that involve personal[1] or sensitive[2] (special category) information (including pseudonymised[3] data) or new technologies to process personal data give rise to privacy issues and concerns. Privacy includes 'confidentiality' and 'patient consent' as an overarching principle, this Policy advocates that respect for patient privacy and dignity must be considered at the outset of any project. To enable organisations to address any privacy concerns and risks, a technique referred to as Data Protection Impact Assessment (DPIA) endorsed by the Information Commissioner's Office (ICO) must be used**.**

It is a requirement of the Data Security and Protection Toolkit that an organisation's 'data protection by design' (see Section 3) procedures ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent and where feasible allows individuals to monitor what is being done with their data. Together the procedures enable an organisation to improve data protection and security. New Systems or Processes should not 'go live' until the 'data protection by design' work has been completed.

The CCG has two main roles within the 'privacy by design' work represented by the DPIA process.

1. The first function is to ensure that as an organisation the CCG ensures its use of personal confidential data (PCD) or patient identifiable data (PID) is lawful[4], appropriate and kept secure. Nationally NHS England through NHS Digital have assessed that CCGs have very little requirement to use PCD or PID in delivering its legal functions. The CCG therefore actively works to reduce and remove all use of PCD / PID within its commissioning and contract management functions.

2. The second function is that as commissioners of services we need to ensure that the providers of these services and systems comply with 'privacy by design' and all legal requirements. The CCG as a commissioner of a service is responsible for the service during its entire lifetime and must ensure that privacy by design is established at the point of commissioning a service and maintained throughout the contracted period of delivery. Monitoring of the 'privacy by design' is undertaken via the CCG's contract management functions with its providers.

[1] See Section 12 (Definitions) Personal Data
[2] See Section 12 (Definitions) Sensitive Personal Data
[3] See Section 12 (Definitions) Pseudonymised Data
[4] See Section 12 (Definitions) Legal Bases for Processing

2 SCOPE

Cambridgeshire and Peterborough Clinical Commissioning Group (the 'CCG') recognises that part of the solution to reducing risk lies in ongoing culture change to ensure that information risk management is high on the agenda and that the DPIA process is advocated as a means of achieving this.

This Policy is, therefore, applicable to any member of staff who is responsible for project managing a new 'project' or 'plans' to modify or procure any system (information asset).

This Policy outlines the CCG's approach and methodology for conducting DPIAs for new and existing systems and processes.

3 DATA PROTECTION BY DESIGN AND DEFAULT

Data Protection by Design and Default gives personal information the same importance in business cases and planning as finance, human resources and capital and physical assets. Information Governance can often be a barrier because data protection and privacy considerations have not been built in from the design of a project.

The CCG has data protection and individuals' privacy built into its business approval and procurement processes ensuring that any concerns are addressed in the early stages of procuring or commissioning any new system, service, product or process. This method guarantees that appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights are in place prior to mobilisation. This will involve but is not limited to:

- Only using Data Processors that provide sufficient guarantees of their technical and organisational measures for data protection by design;
- Anticipating risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals;
- Making data protection an essential component of the core functionality of our processing systems and services.

Important: If a DPIA identifies a high risk that is unable to be mitigated, the CCG must consult the ICO before the Project can go ahead (See Section 9)

DPIA should be seen as a process, rather than just 'filling in a template' and certain information is always required. As a minimum, a DPIA will include:

- A description of the envisaged processing operations and the purposes of the processing (See Appendix 2 – Data Flow Mapping);
- An assessment of:
  (i) the need for and proportionality of the processing;
  (ii) the risks to data subjects (as viewed from the perspective of data subjects);
- A list of the measures envisaged to mitigate those risks and ensure compliance with the GDPR.

DPIAs for business change projects or procurement can be useful to identify efficiencies as well as to support compliance.

A non-exhaustive list of projects that would require a DPIA:

- A new IT system for storing and accessing Personal Confidential Data (PCD).
- A data sharing[5] initiative where multiple organisations seek to link sets of PCD.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing PCD for a new, 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 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.
- Use of data that appears to be pseudonymised or anonymised but could be identifiable if combined with other information. Pseudonymisation is the process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity', and anonymisation is the process of rendering data into a form which does not identify individuals and where identification is not likely to take place'.

4 KEY ROLES AND RESPONSIBILITIES

4.1 CCG Governing Body (GB)

The Governing Body owns the information risk and its implementation.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is responsible to the GB for ensuring Information Risk is developed, implemented, reviewed and its effect monitored. DPIA is one element of the management of information risk. Information risks needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

The SIRO is the key role for identifying and managing risk.

The SIRO will:

- Take ownership of the CCG's information risks;
- Acts as the advocate for information risk on the Governing Body;
- Provide written advice to the Chief Officer on the content of the Statement of Internal Control regarding information risk.

4.3 Data Protection Officer (DPO)

The DPO is responsible for Data Protection compliance within the CCG and 'approves' all full scale DPIAs for recommendation of endorsement to the SIRO. The DPO can provide advice on:

- whether a DPIA is required;
- how the DPIA should be conducted;
- what measures and safeguards can be taken to mitigate risks;

[5] See Section 12 (Definitions) Data Sharing Agreements

- whether the DPIA has been carried out correctly; and
- the outcome of the DPIA and whether the processing can go ahead.

The DPO's advice to Project Managers is recorded on the final version of the full scale DPIA. If you do not follow the DPO's advice, you should record your reasons for not doing so (See Step 7 of the full scale DPIA document) ensuring that you are able to justify your decision and inform the DPO.

The DPO also monitors updates from the project managers regarding the ongoing performance of the DPIA, including how well the planned actions have been implemented to address the risks.

4.4 Information Asset Owners

Information Asset Owners (IAO) are senior individuals (usually Directors) involved in running the relevant business. Their role is to understand:

- what information is held;
- what is added and what is removed;
- how information is moved;
- who has access and why;
- ensure compliance with the relevant legal frameworks, i.e. consent and confidentiality.

Information Asset Owners are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security, confidentiality and integrity and use of the assets. Any Risks identified by the IAO should be added to their Directorate/Team risk register.

Information Asset Owners are responsible for ensuring that DPIAs for the assets they own are maintained throughout the lifetime of a project and for liaising with the Senior ICT Service Development Manager to ensure that their information systems are recorded on the CCG's Information Asset Register.

4.5 Information Asset Administrators

Information Asset Administrators (IAA) support the IAO by ensuring:

- Policies and procedures are followed.
- Recognition of actual or potential security incidents.
- Consultation with their IAO on incident management.
- Information asset registers are accurate and up to date.

These roles are normally undertaken by an operational member of staff who is responsible for one or more information assets reporting to their IAO. Often the 'System Manager'.

4.6 Project Sponsors

The Project Sponsor is the individual (often a senior manager or executive) with overall accountability for the project. The Project Sponsor is primarily concerned with ensuring that the project delivers the agreed business benefits.

4.7 Project Managers

Project Managers must ensure that:

- any project that involves processing of personal data is assessed to identify if a DPIA is required;
- DPIAs are revisited regularly throughout the lifetime of the project to identify any changes made to the proposed use of information i.e. data flow;
- the DPO is consulted, in a timely manner, in all issues relating to the protection of personal data;
- where the CCG has completed a DPIA on behalf of the provider of a service it has commissioned, the 'signed off' DPIA is shared with the provider to enable them to put it through their own formal governance process;
- the DPIA Team are informed of Projects that have been 'abandoned' or put 'on hold'.

4.8 Specialist Advice

Specialist advice can be provided by individuals within the CCG's DPIA Review Team, i.e. Information Governance Team, Senior ICT Service Development Manager; IM&T Clinical Services Manager or the Caldicott Guardian, SIRO and DPO depending on the issues identified as an outcome of completing a full-scale Data Protection Impact Assessment. The Information Governance Function is available to provide the expert knowledge and guidance around the legal framework.

4.9 Staff Responsibilities

All staff employed by the CCG must follow the requirements of this Policy and associated policies, particularly those relating to Information Governance and Data Security. All health professionals must also meet their own professional codes of conduct in relation to confidentiality. Where breaches of confidentiality, security alerts etc are identified relating to an information system, a DPIA must be undertaken to provide assurance that information risk is being managed.

5 PROCESS

Data Protection Impact Assessments must be completed at an early stage of the project or planned modification to an existing process or information asset. Completion of a **DPIA Screening Checklist** during the initial scoping phase of a Project will establish whether your Project is likely to require a **Full Scale DPIA.**

If it is identified that a full scale DPIA is not required for your Project, the Checklist must still be visited at various points in your Project's lifecycle to ensure that there have been no changes made to the proposed use of information, which may impact on whether a Full Scale DPIA is required.

A key aim is to ensure that full compliance with the checklists will be achieved as business processes and rules are specified during the course of the project. The appointed Project Manager is responsible for ensuring that this is carried out with support and guidance from the DPIA Review Team.

Completion of all Data Protection Impact Assessments must be notified to the DPIA Review Team at capccg.infogov@nhs.net to enable the correct level of expertise and support is provided to assist Project Managers with the process.

Summary of the CCG's DPIA Process (See **Appendix 3** for more detail)

Step 1	Project Managers complete their DPIA Screening Checklist in MS Project Online **or** manually by completion of a DPIA Screening Checklist (available on the DPIA page on the Staff Extranet) for projects not managed within MS Project.
Step 2	The DPIA Review Group meet weekly to review all DPIA Screening Checklists and full scale DPIAs received.
Step 3	Following review, the Team will either recommend approval of the Checklist to the CCG's DPO or identify that completion of a full scale DPIA is required. Outcomes of the Group's review are communicated back to the Project Manager and copied to the PMO.
Step 4	Outcomes of the Group's review are recorded within MS Project Online, where applicable.
Step 5	Where a full scale DPIA has been requested, it is recommended that Project Managers seek specialist advice from the CCG's DPIA Review Team at appropriate points during completion of their DPIA.
Step 6	When the DPIA Team have agreed that the DPIA has reached an appropriate point of completion, they will recommend approval to the DPO. The DPO will review the DPIA and contact the Project Lead directly if there are any issues or concerns that need to be addressed prior to sign off. The DPIA is then forwarded by the DPO to the SIRO or their Deputy for sign off. The DPO contacts the Information Asset Owner to request that they liaise with the Senior ICT Service Development Manager to ensure that any assets are added to the CCG's Information Asset Register.

Occasionally, during the 'sign off' process, a Project implementation action plan may be required, this will be devised for initial approval and subsequent auditing and monitoring by the Project team. The Project team are responsible for the implementation of this Plan. This ensures that information risks are recorded, mitigation put in place with an annual review scheduled to ensure ongoing compliance with confidentiality, data protection and security.

6 SUPPORT AND TRAINING

The CCG's DPIA Review Team has varied areas of expertise and is available to offer support and guidance to Project Managers and Information Asset Owners in completing Data Protection Impact Assessments. Further information and guidance is available on the CCG's DPIA staff extranet page here.

The CCG will periodically provide DPIA Training Workshops for staff whose roles involve project management, the objectives of the training provision are:

- To improve staff knowledge of the importance of DPIAs;
- To provide an opportunity for staff to develop skills in completing Data Flow Maps and full scale DPIAs;
- To provide an opportunity for staff to ask questions on DPIA;
- To improve understanding and confidence in completing DPIA in the future;
- To improve the CCG's DPIA process'.

7 STATEMENT OF INTENT

Compliance with confidentiality and data protection must be taken into account and there must also be a comprehensive consideration of potential impacts on information quality at the design phase of any new process or information assets. Some of the considerations that must be taken into account are whether a new (or modified) project /process or information asset will:

- ensure that the necessary consents have been obtained from those whose personal data is being used, where appropriate;
- effect the quality of personal information already collected;
- allow personal information to be checked for relevancy, accuracy and validity
- incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required in line with Department of Health retention and destruction guidelines;
- have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction, breaches of confidentiality or damage;
- enable data retrieval to support business continuity in the event of emergencies or disasters;
- enable the timely location and retrieval of personal information to meet subject access requests;
- alter the way in which the organisation records in or monitors and reports information from a key organisational system and what such a change will mean for the information and the service.

8 ESCALATION

Where the DPIA Review Team consider it necessary, any DPIA can be escalated to the CCG's Head of PMO; SIRO or DPO. Such situations may include:

- A provider failing to acknowledge the Information Governance and Security requirements of the Data Security and Protection Toolkit;
- A Project Manager not responding to the DPIA Review Team's request for a full scale DPIA;
- A Project Manager not responding to the DPIA Review Team's revision comments or requests for further information;
- A Project Manager not complying with an agreed Project Implementation Action Plan.

9 CONSULTING THE ICO

If we have carried out a full scale DPIA that identifies a high risk, and we are unable to implement measures to reduce this risk, the CCG may need to consult with the Information Commissioner's Office (ICO). This might mean that you cannot go ahead with the Project until we have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, we may not need to consult the ICO.

10 PUBLISHING DPIAs

Although publishing a DPIA is not a requirement of GDPR, the ICO recommends that, where possible, organisations should actively consider the benefits of publication (removing sensitive details if necessary). As well as demonstrating compliance, publication can help engender people's trust and confidence in organisation's whose services they use.

Assertion 1.6.13 of the Data Security and Protection Toolkit i.e. 'Data Protection Impact Assessments are published and available as part of the organisation's transparency materials' is not currently a 'Mandatory' required, however, in time this could change.

11 MONITORING COMPLIANCE WITH THIS POLICY

Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual responsible for the monitoring**	**Frequency of the monitoring activity**	**Group / committee which will receive the findings / monitoring report**	**Group / committee / individual responsible for ensuring that the actions are completed**
Review of the CCG's Information Assets	Risk Assessment by Information Asset Owners	CCG's Senior ICT Service Development Manager	Annually	IG, BI and IM&T Steering Group	CCG Senior Information Risk Owner (SIRO)
DPIAs for the introduction of new systems or planned modification to existing processes or information assets	Review by the DPIA Review Group	CCG IG Lead / DPO	Weekly	IG, BI and IM&T Steering Group	CCG Data Protection Officer (DPO)

12 DEFINITIONS

Data (Information) Sharing Agreements	Data sharing agreements set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These often form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis. *Source: ICO Data Sharing Code of Practice*
Personal Data	Often referred to as PCD (personal confidential data) or PID (patient identifiable data). Defined by the General Data Protection Regulations (GDPR) as data that is capable of identifying a living individual, but isn't classified as sensitive data, i.e. name; GP; next of kin; address; postcode; date of birth or any online identifier (e.g. an IP address). **Note: For legitimate processing of Personal Data in accordance with the terms of the GDPR - see Appendix 1)**
Sensitive Personal (Special Category) Data	Defined under the General Data Protection Regulations (GDPR) as 'special categories of personal data' e.g. data such as patient diagnosis; physical or mental health and condition; ethnicity; sexual life; religious beliefs. Also includes genetic data, and biometric data and facial recognition where processed to uniquely identify an individual. **Note: For legitimate processing of Sensitive Personal Data in accordance with the terms of the GDPR - see Appendix 1)**
Pseudonymised Data	Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example, a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention. **Note: Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a specific individual.**
Legal Basis for Processing (See Appendix 1)	The General Data Protection Regulation (GDPR) requires organisations to record a legal basis for all personal data that they are processing. Individuals have a right to be informed about processing of their personal data, and should, wherever possible be given a choice over processing (i.e. consent processes).

13 STATUTORY AND NATIONAL GUIDANCE

This following statutory and national guidance has been used to develop this document:

Data Protection Act 2018
Data Protection Impact Assessments (ICO Website)
Data Protection Impact Assessments (DPIA) (ICO Guidance)
Guide to the General Data Protection Regulation (ICO Guidance)
Data Sharing Code of Practice (ICO Guidance)

This Policy meets the requirements of the National Data Guardian's Data Security Standard 1; Assertion 1.6 of NHS Digital Data Security and Protection Toolkit i.e. 'The use of personal information is subject to data protection by design and by default'

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Equality Impact Assessment Form

Name of Proposal (policy/strategy/function/ service being assessed)	CCG Data Protection Impact Assessment Policy and Procedure
Those involved in assessment:	Policy developed in consultation with the IG, BI & IM&T Steering Group and for endorsement by the Integrated Performance and Assurance Committee
Is this a new proposal?	Yes. New Policy and Procedure document translated from the CCG's DPIA Process Guidance. Policy developed in accordance with new guidance under the Data Protection Act 2018.
Date of Initial Screening:	May 2019

1. What are the aims, objectives?	This Policy will ensure that as an organisation the CCG ensures its use of personal confidential data (PCD) or patient identifiable data (PID) is lawful appropriate and kept secure. As commissioners of services the CCG also needs to ensure that the providers of services comply with 'privacy by design' and all other legal requirements.
2. Who will benefit?	All staff, service users
3. Who are the main stakeholders?	Staff, PMO, patients/service users, service providers
4. What are the desired outcomes?	Staff awareness of the policy Recognition of the legal requirement for completion of Data Protection Impact Assessments for projects.
5. What factors could detract from the desired outcomes?	Lack of awareness of the existence of the Policy. Failure to follow the Policy.
6. What factors could contribute to the desired outcomes?	Knowledge of the policy and implementation
7. Who is responsible?	All staff, Project Managers

8. Have you consulted on the proposal? If so with whom? If not why not?	Policy developed in consultation with the IG, BI and IM&T Steering Group for approval and endorsement by the Integrated Performance and Assurance Committee

9. **Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)**		Yes	No
Age	Consider: Elderly, or young people		x
Disability	Consider: Physical, visual, aural impairment, Mental or learning difficulties		x
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned		x
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		x
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related mater		x
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		x
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		x
Sex /Gender	Consider: Male and Female		x
Sexual Orientation	Consider: Know or perceived orientation		x

10. **What information and evidence do you have about the groups that you have selected above**?

The above protected characteristics will have no adverse impact as the Policy has been developed in accordance with new Data Protection legislation (ie General Data Protection Regulation May 2018).

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People

Examples of impact re given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

Please list the positive and negative impacts you have identified in the summary table on the following page.

Summary	
Positive impacts (note the groups affected) N/A	Negative impacts (note the groups affected) N/A

Summarise the negative impacts for each group:

N/A

11. **What consultation has taken place or is planned with each of the identified groups?**

Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group prior to endorsement by the Integrated Performance and Assurance Committee.

What was the outcome of the consultation undertaken?

Approval and endorsement sought

12. **What changes or actions do you propose to make or take as a result of research and/or consultation?**

Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided. The Information Governance Team on behalf of the Associate Director of Corporate Affairs will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

12.1 **Will the planned changes to the proposal?** Please State Yes or No

a) Lower the negative impact?	N/A
b) Ensure that the negative impact is legal under anti-discriminatory law?	N/A
c) Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	N/A

13. **Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits**.

Information risk **-** The CCG must respect patient confidentiality in accordance with the NHS Constitution, ICO Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of PCD during the deployment of projects.

14. **What monitoring/evaluation/review systems have been put in place?**

Monitoring will be undertaken by the Information Governance Team. The frequency of review will be carried out every other year or as required.

15. **When will it be reviewed?**

May 2021

Date completed:	16 May 2019
Signature:	IG Administrator
Approved by:	Equality and Diversity Advisor
Date approved:	28 May 2019

Appendix 1 – Lawful Bases for Processing Personal Data under GDPR

The General Data Protection Regulation (GDPR) requires that a lawful basis for processing **personal data** (GDPR Article 6) is identified before any processing commences. Where **special category data** (GDPR Article 9) is processed, a lawful basis **and** a separate condition must be identified

Whilst GDPR provides many more conditions for processing than the Data Protection Act 1998, it is less prescriptive as to how those conditions are met, but for the purposes of this document, relevant provisions are that:

- Organisations must document a legal basis for processing personal data.
- Individuals have a right to be informed about processing of their personal data and should be given choice over processing wherever possible (consent processes).

Consent is only one of the legal bases for processing personal information. Organisations, particularly public authorities or other providers of publicly funded services may be legally obliged to process personal data by legislation other than data protection, which means that consent cannot apply, and should not be sought.

GDPR Article 6 - Lawfulness of processing personal data
(Article 6(1); Article 6(2) and Recital 40)

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;

(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
(Note: This basis does not apply to public authorities who process data to enable them to perform their official tasks.)

GDPR – Article 9(2) Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Appendix 2 – Data Flow Mapping

As part of the DPIA process, a description of how information is collected, stored, used, retained and deleted should be included. We should also explain what information is used, what it is used for and who will have access to it.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information will be used in a project. An incomplete understanding of how information is used can be a significant privacy risk e.g. data might be used for unfair purposes or disclosed inappropriately.

This part of the DPIA process can be integrated with any similar exercises which may already be in place, e.g. conducting information audits, developing information maps and using information asset registers.

A **Data Flow Map** (See example p14) is a graphical representation of the flows of data and should include:

- All incoming and outgoing data (the organisations and / or people sending / receiving the data);
- The legal basis for each flow;
- The type and volume of data being transferred;
- The secure method of transfer (i.e. Systems being used);
- Storage for the 'Data at Rest' i.e. System, filing cabinet;

If the data has already been captured covering the proposed project or similar document this can be useful for understanding how personal data might be used.

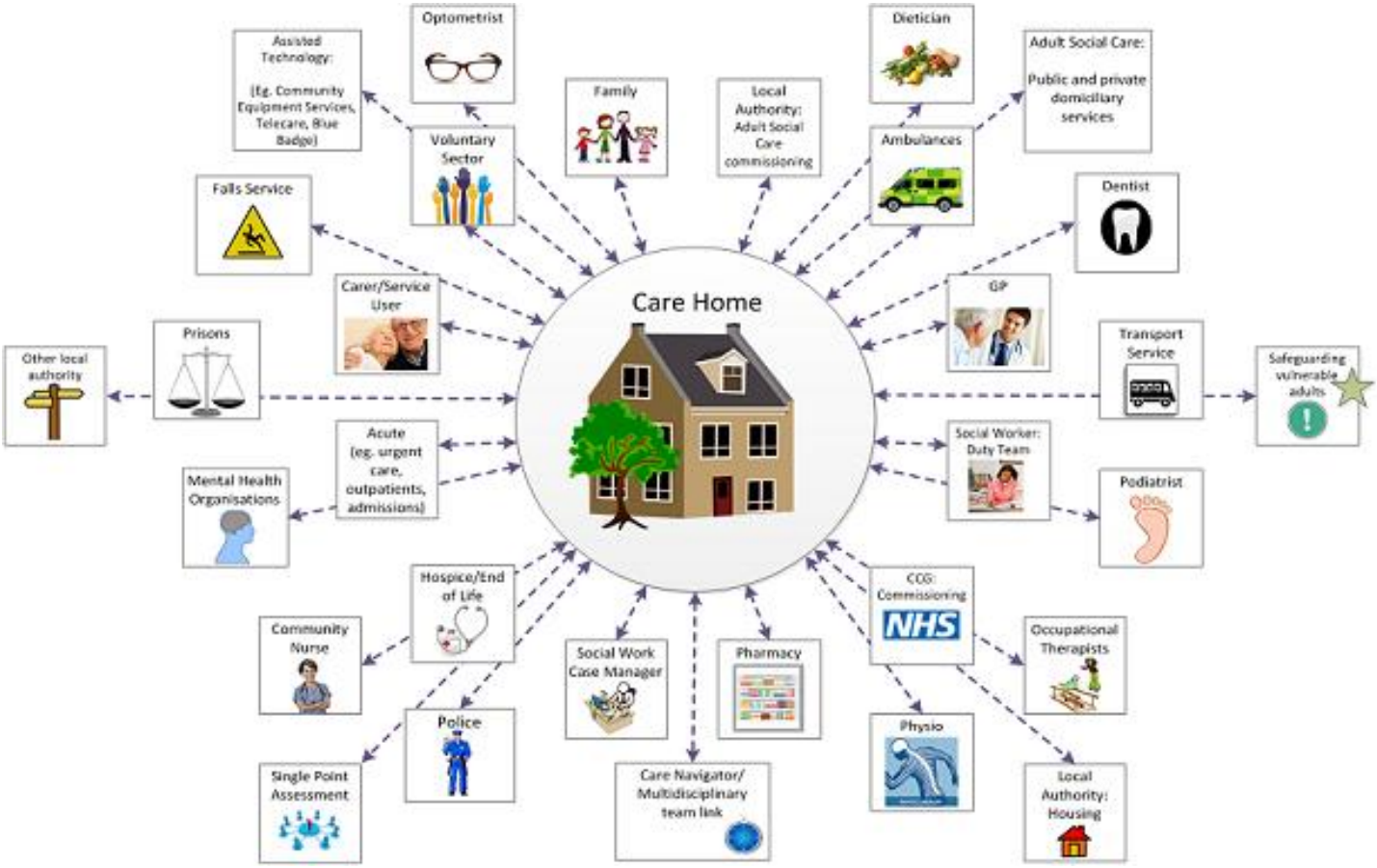
The information flows can be recorded as a flowchart, an information asset register or a project design brief which can then be used as an important part of the final DPIA.

Describing information flows

- Explain how information will be obtained, used and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' (unforeseen or unintended uses of the data e.g. data sharing).
- People who will be using the information are consulted on the practical implications.
- Potential future uses of information are identified, even if they are not immediately necessary.

Example – Care Provider Data Flow Map

For each data flow the **legal basis** (See Appendix 1) for the flow, the **type and volume** of data being **transferred** and the **secure method of transfer** (i.e. Systems being used) would need to be identified.



Source: NHS Digital

Appendix 3 – DPIA Administration Standard Operating Procedure

STANDARD OPERATING PROCEDURE
Data Protection Impact Assessment (DPIA) Administration

INTRODUCTION

All new projects, processes and systems (including software and hardware) which are introduced must comply with confidentiality, privacy and data protection requirements. Data Protection Privacy impact assessments (DPIAs) are a tool, which can help the CCG, identify the most effective way to comply with these requirements and to fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

DOCUMENT CONTROL

Version	Date	Amendment History
1.0	26/05/2016	Initial draft
1.1	25/07/2016	In addition to the Project Manager, the Project Sponsor is to be notified of a DPIA's approval and any resulting recommendations / action plan to ensure accountability.
1.2	07/11/2016	Update to the approval DPIA approval process following the introduction of WAVE and subsequent changes to the PMO process.
1.3	30/03/2017	Updated in line changes in the process following the use of Wave for review of DPIA Screening Checklists
1.4	28/02/2018	Updated in line with changes in the process following the use of Microsoft Project Online. PIA replaced with DPIA in preparation for the introduction of GDPR
1.5	05/06/2018	Updated following the implementation of General Data Protection Regulation (GDPR)
1.6	10/10/2018	Amended to reflect the approval process to include DPO and SIRO sign off and DPO responsibility to request that the IAO adds any assets to the CCG's Information Asset Register.

PROCEDURE

The following procedure has been developed to enable Cambridge and Peterborough CCG to standardise the DPIA process:

- The IG Team admin will obtain the DPIA Screening Checklist/s that require review by filtering projects within Microsoft Project online i.e. DPIA Screenings for Review and notify the DPIA Review Group of the projects requiring review on MS Project Online.

- Details of all DPIA Screening Checklists for review are stored in the DPIA folder on the Corporate Services Drive within SharePoint.

- Create a folder in the mailbox on outlook for new projects (new email updates).

- Create a folder on the drive for updates and actions received initially for the storage/accessibility of versions of DPIA Screening Checklists/full scale DPIAs. Emails trails to be saved with in the folder for reference/records.

- Log details for the Project along with their status on the DPIA Master Log.

- A link to the full scale DPIA is sent to members of the Review Team for comments which are made within the document for response by the Project Manager.

- DPIA checklists /documents discussed in weekly review meetings to be attended by members of the DPIA Review Group (listed on page 2).

- Comments from members of the Review Group will only be sent to the Project Manager once agreed/discussed with the wider Group. Once agreed, the project contact will be notified for them to respond to the comments stating what action has been taken etc.

- Make notes of any issues and recommendations discussed in review meeting and record in the DPIA log.

- If there are any 'Yes' answers to the Screening Checklist questions, then the project will require a DPIA. Of note is an affirmative answer to question one regarding the use of PID (including pseudonymised data). In this case, the Project Lead can be informed to complete a full scale without consulting the wider Group.

- Once a DPIA Screening Checklist has been approved/not approved, ensure that the status of the project is updated on Project Online by updating the DPIA screening tab with the decision as agreed by members of the Group as to whether a full DPIA will be required or not.

- Record any significant changes on the DPIA Master Log and label updates (for example v1.1, v1.2) to ensure version control.

- Ensure that DPIA Master Log has details on DPIA/DPIA Screening Checklist Reference number, Date Submitted, Date Acknowledged, Project Lead,

Project Name/Workstream, Project Description, Projected Go Live Date, Updates/Actions, Recommendations/Actions Plan, Status and Approval on the respective tabs in the log.

- As meetings take place and updates are communicated, ensure email folder, drive folder and DPIA Master Log is updated.

- If the project is on hold, awaiting confirmation, abandoned, superseded, or at Screening Checklist stage, record on the appropriate tab on the Master Log.

- DPIAs approved by the DPIA Review Group will subsequently be sent to the CCG's Data Protection Officer for sign-off. The DPO will assess the document and contact the Project Lead directly if there are any issues/concerns that require addressing prior to sign off. Once all issues have been resolved, the DPO will send the DPIA to the SIRO or their Deputy for endorsement.

- Following SIRO endorsement, the DPO is responsible for informing the Information Asset Owner of the requirement to liaise with the Senior ICT Service Development Manager to ensure that any assets are added to the CCG's Information Asset Register.

- The IG administrator will then send notification of approval to the PMO Team via their generic mailbox (CAPCCG.PMO@nhs.net).

- Upon approval of a DPIA, update the DPIA Master Log, ensuring Recommendations/Actions required prior to 'Go Live'/ during project implementation are entered accordingly and highlighted in RED on the log.

- Final version of the DPIA to be saved in PDF format and forwarded to the **Project Lead** and **Project Sponsor** (ensuring accountability) notifying of the approval and any conditions to the approval i.e. Recommendations / Action Plan to be completed prior to /during implementation.

The CCG's DPIA Review Team has varied areas of expertise to help Project Managers in completing their DPIAs. The following staff roles form the CCG's DPIA Review Team whose responsibilities are reviewing DPIAs and getting them to a point where it is appropriate to recommend DPO approval.
Information Governance Lead / DPO
Information Governance Support Manager / DPIA Co-ordinator
Senior ICT Service Development Manager
Strategic Clinical Services IM&T Consultant
Primary Care Clinical Services IT Manager
Clinical Services IM&T Development Manger
Choice, Choose & Book Manager
ICT Clinical Services Facilitator
The Corporate Services Administrator (IG) is responsible for maintaining the DPIA log and administration of the DPIA process.