Bradford City Clinical Commissioning Group
Bradford Districts Clinical Commissioning Group

Privacy Impact Assessment Procedure and IG Checklist

Procedure approved by: Joint Audit and Governance Committee

Date: December 2016

Next Review Date: September 2018

Version: 2.0

Review and Amendment Log / Control Sheet

Responsible Officer:	**Chief Officer**
Clinical Lead:	
Author:	Senior IG Specialist eMBED
Date Approved:	
Committee:	
Version:	2.0
Review Date:	30 September 2016

Version History

Version	Date	Author	Description	Circulation
1.0	12 September 2014	IG Specialist YHCS	Initial Draft	Joint Audit and Governance Committee
2.0	30 September 2016	Senior IG Specialist eMBED	Revisions throughout to: • Structure • Grammar • Language • Development of PIA suite of supporting documents to assist organisations when completing a PIA.	

Contents

1. Introduction

Privacy Impact Assessments (hereafter known as PIA) serve to ensure that the organisation remains compliant with legislation and NHS requirements such as the information governance toolkit, which determine the use of Personal Confidential Data (PCD). The information governance checklist and PIA have been developed to provide an assessment prior to new services or new information processing/sharing systems being introduced. They are less effective when key decisions have already been taken.

PIA's identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow for the identification and remedy of problems at an early stage, reducing potential distress, subsequent complaints and the associated costs and damage to reputation which might otherwise occur.

A PIA aids an organisation in determining how a particular project, process or system will affect the privacy of the individual. It is important to consider whether a PIA is required once you know what it is you are hoping to achieve, what you will require to get there and how you plan to go about doing it.

Conducting a PIA does not have to be complex or time consuming.

2. Privacy Impact Assessments

PIAs help identify privacy risks, foresee problems and bring forward solutions. A successful PIA will:

- identify and manage risks (see Appendix A for examples)
- avoid inadequate solutions to privacy risks
- avoid unnecessary costs
- avoid loss of trust and reputation
- inform the organisation's communication strategy
- meet or exceed legal requirements

The Information Commissioners Office (ICO) has produced guidance materials on which this procedure is based (see Appendix C).

Consideration as to whether a PIA should be completed is mandated through the information governance toolkit. PIAs ensure that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable information.

3. Purpose of a PIA

A PIA should serve to:

- identify privacy risks to individuals

- identify privacy and data protection compliance liabilities
- protect the organisations reputation
- instil public trust and confidence in your project/product
- avoid expensive, inadequate "bolt-on" solutions
- inform your communications strategy

Following review of the screening questions (Annex A) it may be decided that a PIA is required. Where it is thought that a PIA is required, Annex B should be completed and submitted to the information governance team for a preliminary review. It is recommended that IG Team review is sought prior to the final PIA being submitted to the Joint Audit and Governance Committee, SIRO or Caldicott Guardian.

4. Responsibilities

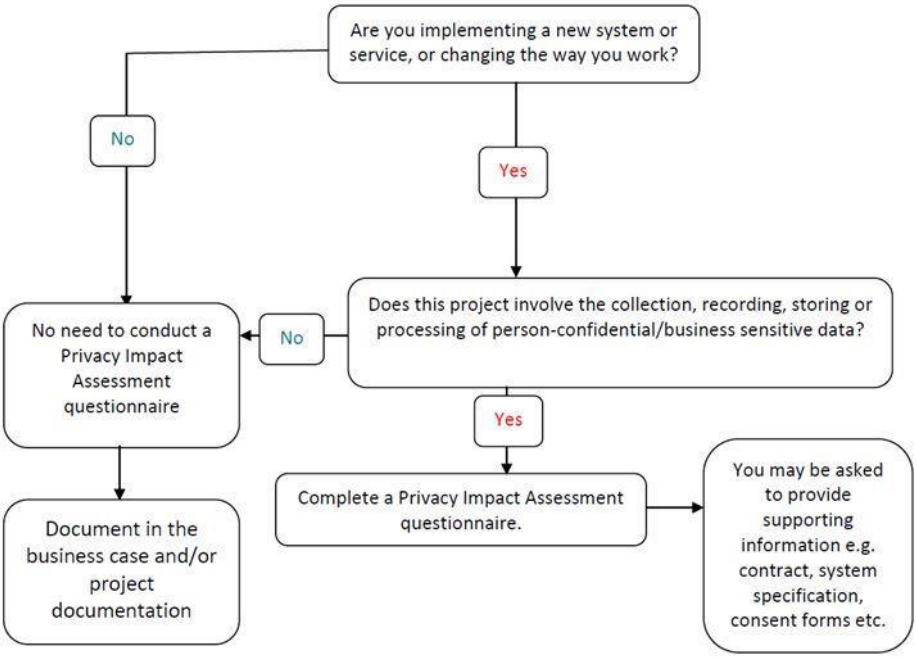
Responsibility for ensuring that a PIA is considered and if appropriate, completed, resides with managers leading the introduction of new systems, sharing or projects.

Line managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of the PIA procedure.

There is an expectation that partner organisations involved in supplying/providing services should provide technical information for the PIA, where this is otherwise unclear.

This guidance therefore applies to all staff and all types of information held by the organisation. Further details of responsibilities are to be found in the organisation's policies and procedures.

5. Is a PIA required for every project?



The ICO envisages PIAs being used where a project includes the use of personal data, where there otherwise a risk to the privacy of the individual, utilisation of new or intrusive technology, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and 'unexpected' way. The screening questions (see Annex A) help determine if a PIA is required.

6. When should I start a PIA?

PIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed
- you know what you want to do
- you know how you want to do it
- you know who else is involved

It **must** be completed before:

- decisions are set in stone
- you have procured systems
- you have signed contracts/memorandum of understanding/agreements
- while you can still change your mind

7. Publishing PIA's

All PIA's are to be included within the organisation's publication scheme and must therefore be presented to the head of communications once they have received approval.

It is acknowledged that PIA's may contain commercial sensitive information such as security measures or intended product development. It is acceptable for such items to be redacted but as much of the document should be published as possible given all information within a public organisation can be requested through the Freedom of Information Act and will be listed in the publication scheme.

8. Related CCG Policies

Access to Records under DPA Procedure
Business Continuity Plan
Confidentiality and Data Protection Policy
E mail Policy
Freedom of Information and EIR Policy
Freedom of Information Procedures
IG Strategic Vision, Policy and Framework
Incident Reporting Policy
Information Security Policy
Interagency Information Sharing Protocol
Internet and Social Media Policies
Network Security Policy
Privacy Impact Assessment procedure
Records Management and Information Lifecycle Policy
Remote access and home working procedures
Risk Management Policy

Safe Haven Guidelines and Procedure

Privacy Impact Assessment (PIA) Screening Questions

The below screening questions should be used inform whether a PIA is necessary. This is not an exhaustive list therefore in the event of uncertainty completion of a PIA is recommended.

Project title	Click here to enter text.
Brief description	Click here to enter text.

Screening completed by

Name	Click here to enter text.
Title	Click here to enter text.
Department	Click here to enter text.
Email	Click here to enter text.
Review date	Click here to enter text.

Marking any of these questions is an indication that a PIA is required:

Screening Questions		**Tick**
1	Will the project involve the collection of new identifiable or potentially identifiable information about individuals?	☐
2	Will the project compel individuals to provide information about themselves? i.e. where they will have little awareness or choice.	☐
3	Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?	☐
4	Are you using information about individuals for a purpose it is not currently used for or in a new way? i.e. using data collected to provide care for an evaluation of service development.	☐
5	Where information about individuals is being used, would this be likely to raise privacy concerns or expectations? i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress.	☐
6	Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	☐
7	Will the project result in you making decisions in ways which can have a significant impact on individuals? i.e. will it affect the care a person receives.	☐
8	Does the project involve you using new technology which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition or automated decision making.	☐
9.	Is a service being transferred to a new supplier (recontracted) and the end of an existing contract	☐
10.	Is process being moved to a new organisation (but with same staff and processes)	☐

Please retain a copy of this questionnaire within your project documentation.

Please note that once completed the following sections (1 to 3) should be detached from the remaining document prior to being included in the CCGs Publication Scheme.

Privacy Impact Assessment (PIA)

Please complete all questions with as much detail as possible and then contact the IG Team prior to seeking approval.

Section 1: System/Project General Details

Project title:	Click here to enter text.	
Objective:	Click here to enter text.	
Background: Why is the new system/change in system required? Is there an approved business case?	Click here to enter text.	
Relationships: For example, with other Trust's, organisations.	Click here to enter text.	
Other related projects:	Click here to enter text.	
Project Manager:	Name:	Click here to enter text.
	Title:	Click here to enter text.
	Department:	Click here to enter text.
	Telephone:	Click here to enter text.
	Email	Click here to enter text.
Information Asset Owner: All information systems/assets must have an Information Asset Owner (IAO). IAO's should normally be a Head of Department/Service.	Name:	Click here to enter text.
	Title:	Click here to enter text.
	Department:	Click here to enter text.
	Telephone:	Click here to enter text.
	Email	Click here to enter text.
Information Asset Administrator: Information systems/assets may have an Information Asset Administrator (IAA) who reports the IAO. IAA's are normally System Managers/Project Leads.	Name:	Click here to enter text.
	Title:	Click here to enter text.
	Department:	Click here to enter text.
	Telephone:	Click here to enter text.
	Email	Click here to enter text.
Customers and other stakeholders:	Click here to enter text.	

Section 2: Privacy Impact Assessment Key Questions

	Question	Response
Data Items		
1.	**Will the system/project/process (referred to thereafter as 'project') contain identifiable or Personal Confidential Data (PCD)?** If answered 'No' then a PIA is not required.	☐ Yes ☐ No If yes, who will this data relate to: ☐ Patient ☐ Staff ☐ Other: Click here to enter text.
2.	**Please state purpose for the collection of the data:** For example, patient care, commissioning, research, audit, evaluation.	Click here to enter text.
3.	**Please tick the data items that are held in the system** **Personal** **Sensitive**	☐ Name ☐ Address ☐ Post Code ☐ Date of Birth ☐ GP Practice ☐ Date of Death ☐ NHS Number ☐ NI Number ☐ Medical History ☐ Trade Union membership ☐ Political opinions ☐ Religion ☐ Ethnic Origin ☐ Sexuality ☐ Criminal offences ☐ Other:
4.	**What consultation/checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this project?**	Click here to enter text.
5.	**How will the information be kept up to date and checked for accuracy and completeness?**	Click here to enter text.
Data processing		

	Question	Response
6.	**Will a third party be processing data?**	☐ Yes ☐ No If no, please go to the Confidentiality section.
7.	**Is the third party contract/supplier of the project registered with the Information Commissioner?**	☐ Yes ☐ No Organisation: Click here to enter text. Data Protection Registration Number: Click here to enter text.
8.	**Has the third party supplier completed an Information Governance Toolkit Return?**	☐ Yes ☐ No If yes, please give organisation code and percentage score: Click here to enter text. *IG Toolkit Score:* ☐ Satisfactory ☐ Unsatisfactory If unsatisfactory, please request a copy of the improvement plan and provide it with this assessment.
9.	**Does the third party/supplier contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** See CCG Contract and Commissioning Information Governance Assurance checklist.	☐ Yes ☐ No
10.	**Will other third parties (not already identified) have access to the project?** Include any external organisations.	☐ Yes ☐ No If so, for what purpose? Click here to enter text. Please list organisations and by what means of transfer: Click here to enter text.
Confidentiality		
11.	**Please outline what privacy/fair processing notices and leaflets will be provided.** A copy of the privacy/fair processing notice and leaflets must be provided.	Click here to enter text.
12.	**Does the project involve the collection of data that may be unclear or intrusive?** Are all data items clearly defined? Is there a wide range of sensitive data being included?	☐ Yes ☐ No

	Question	Response
13.	**Are you relying on individuals (patients/staff) to consent to the processing of personal identifiable or sensitive data?**	☐ Yes ☐ No If yes, what type of consent will be sought? ☐ Explicit ☐ Implicit How will that consent be obtained and by whom? Click here to enter text. If no, which legal basis/justification is being used instead? ☐ Medical purpose ☐ Public Interest ☐ Court Order ☐ Other: Click here to enter text.
14.	**How will consent, non-consent, objections or opt-outs be recorded and respected?**	Click here to enter text.
15.	**Will the consent cover all processing and sharing/disclosures?**	☐ Yes ☐ No If not, please detail: Click here to enter text.
16.	**What process is in place for rectifying/blocking data?** What would happen if such a request were made?	Click here to enter text.
Engagement		
17.	**Has stakeholder engagement taken place?**	☐ Yes ☐ No If yes, how have any issues identified by stakeholders been considered? Click here to enter text. If no, please outline any plans in the near future to seek stakeholder feedback: Click here to enter text.
Data Sharing		
18.	**Does the project involve any new information sharing between organisations?**	☐ Yes ☐ No If yes, please describe: Click here to enter text. **Please provide a data flow diagram.**
Data Linkage		

	Question	Response
19.	**Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?** The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously)	☐ Yes ☐ No If yes, **please provide a data flow diagram.**
Information Security		
20.	**Who will have access to the information within the system?** Please refer to roles/job titles.	Click here to enter text.
21.	**Is there a useable audit trail in place for the project?** For example, to identify who has accessed a record?	☐ Yes ☐ No ☐ Not applicable If yes, please outline the audit plan: Click here to enter text.
22.	**Describe where will the information be kept/stored/accessed?**	Click here to enter text.
23.	**Please indicate all methods in which information will be transferred**	☐ Fax ☐ Email (Unsecure/Personal) ☐ Email (Secure/nhs.net) ☐ Internet (unsecure – e.g. http) ☐ Telephone ☐ Internet (secure – e.g. https) ☐ By hand ☐ Courier ☐ Post – track/traceable ☐ Post – normal ☐ Other: Click here to enter text.
24.	**Does the project involve privacy enhancing technologies?** Encryption; 2 factor authentication, new forms of pseudonymisation.	☐ Yes ☐ No If yes, please give details: Click here to enter text.
25.	**Is there a documented System Level Security Policy (SLSP) or process for this project?** A SLSP is required for new systems.	☐ Yes ☐ No If yes, please provide a copy.
Privacy and Electronic Communications Regulations		

	Question	Response
26.	**Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?** Please note that seeking to influence an individual is considered to be marketing.	☐ Yes ☐ No If yes, what communications will be sent? Click here to enter text. Will consent be sought prior to this? ☐ Yes ☐ No
Records Management		
27.	**What are the retention periods for this data?** Please refer to the Records Management: NHS Code of Practice.	Click here to enter text.
28.	**How will the data be destroyed when it is no longer required?**	Click here to enter text.
Information Assets and Data Flows		
29.	**Has an Information Asset Owner been identified and does the Information Asset Register require updating?**	☐ Yes ☐ No If yes, include a complete Information Asset Register New Entry Form.
30.	**Have the data flows been captured?**	☐Yes ☐No If yes, include a complete Information Asset Register New Entry Form.
Business Continuity		
31.	**Have the requirements for business continuity been considered?**	☐ Yes ☐ No If yes, please detail: Click here to enter text.
Open Data		
32.	**Will (potentially) identifiable and/or sensitive information from the project be released as Open Data (be placed in to the public domain)?**	☐ Yes ☐ No If yes, please describe: Click here to enter text.
Data Processing Outside of the EEA		

	Question	Response
33.	**Are you transferring any personal and/or sensitive data to a country outside the European Economic Area (EEA)?**	☐ Yes ☐ No If yes, which data and to which country? Click here to enter text.
34.	**Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?**	☐ Not applicable ☐ Yes ☐ No If yes, who completed the assessment? Click here to enter text.

Section 3: Review and Approval

Assessment completed by

Name:	Click here to enter text.
Title:	Click here to enter text.
Sent electronically or Signed:	☐
Date:	Click here to enter text.

Assessment reviewed (IG) by

Name:	Click here to enter text.
Title:	Click here to enter text.
Reviewed electronically or Signed:	☐ Endorsement by IG Subject Matter Expert is attached.
Date:	Click here to enter text.

Information Governance Approval from the Joint Audit and Governance Committee, SIRO or Caldicott Guardian

Name:	Click here to enter text.
Title:	Click here to enter text.
Electronic Approval or Signed	☐ The Information Governance Approval is attached.
Date:	Click here to enter text.

Appendix A - Example risks

Risks to individuals

i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
ii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
iii. New surveillance methods may be an unjustified intrusion on their privacy.
iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
vi. Identifiers might be collected and linked which prevent people from using a service anonymously.
vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
viii. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
x. If a retention period is not established information might be used for longer than necessary.

Corporate risks

i. Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
ii. Problems which are only identified after the project has launched are more likely to require expensive fixes.
iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
iv. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
vi. Data losses which damage individuals could lead to claims for compensation.

Compliance risks

i. Non-compliance with the DPA.
ii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
iii. Non-compliance with sector specific legislation or standards.
iv. Non-compliance with human rights legislation.

Appendix B - Glossary

Item	*Definition*
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Caldicott	Seven Caldicott Principles were established following the original reviewed in 1997 and further development in 2013. The principles include: 1. justify the purpose(s) 2. don't use patient identifiable information unless it is necessary 3. use the minimum necessary patient-identifiable information 4. access to patient identifiable information should be on a strict need-to-know basis 5. everyone with access to patient identifiable information should be aware of their responsibilities 6. understand and comply with the law 7. the duty to share information can be as important as the duty to protect patient confidentiality
Data Protection Act 1998	This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: 1. be processed fairly and lawfully. 2. be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. 3. be adequate, relevant and not excessive. 4. be accurate and current.

5. not be retained for longer than necessary.
6. be processed in accordance with the rights and freedoms of data subjects.
7. be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.
8. not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.

European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.

Information Risk	An identified risk to any information asset that the organisation holds. Please see the Risk Policy for further information.
Personal Data	This means data which relates to a living individual which can be identified: 1. from those data, or 2. from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Pseudonymisation	Where patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after

	the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Sensitive Data	This means personal data consisting of information as to the: A. racial or ethnic group of the individual B. the political opinions of the individual C. the religious beliefs or other beliefs of a similar nature of the individual D. whether the individual is a member of a trade union E. physical or mental health of the individual F. sexual life of the individual G. the commission or alleged commission by the individual of any offence H. any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board

Appendix C - Further information

Relevant statutory legislation and law:

Common Law Duty of Confidentiality
Data Protection Act 1998
Freedom of Information Act 2000
General Data Protection Regulations 2016
Human Rights Act 1998
Privacy and Electronic Communications Regulations 2003

Further reading and guidance:

Caldicott 2 Review Report and Recommendations
Confidentiality Code of Practice
HSCIC Code of practice on confidential information
Information Security Code of Practice
Records Management Code of Practice
The ICO's Anonymisation: managing data protection risk code of practice may help identify privacy risks associated with the use of anonymised personal data.
The ICO's Data sharing: code of practice may help to identify privacy risks associated with sharing personal data with other organisations.
The ICO's Privacy Notices: Code of Practice.