NHS
Harrogate and Rural District
Clinical Commissioning Group

Privacy/Data Protection Impact Assessment Procedure

November 2017

Authorship:	**John Robinson,** **Embed Health Consortium**
Committee Approved:	Audit Committee
Approved date:	November 2017
Review Date:	November 2020
Equality Impact Assessment:	Completed
Target Audience:	Council of Members, Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	032
Version Number:	3.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

Version	Date	Author	Description	Circulation
0.1	12 September 2014	WSYBCSU	Initial Draft	IG Committee
2	12 August 2015	YHCS	Minor revisions and clarifications added	IG Committee
2.1a	30 September 2016	Embed	Revisions throughout to: Structure Grammar Prompts Language Development of PIA suite of supporting documents to assist organisations when completing a PIA.	IG Committee
2.1b	7 November 2016	Embed	Minor revisions to wording for screening contact details.	IG Committee
3.0	November 2017	Embed	Updated to reference requirements under: • General Data Protection Regulation, • Information Commissioners Office Guidance, and • Reference to the Records Management Code of Practice Health and Social Care 2016	Audit Committee November 2017

Contents

1. Introduction

Privacy Impact Assessments (PIAs) [1]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)[2]. PIAs aid organisations in determining how a particular project, process or system will affect the privacy of the individual. The PIA Screening Questions and Privacy Impact Assessment have been developed to provide an assessment *prior to* new services or new information processing/sharing systems being introduced. a The PIA is less effective when key decisions have already been taken.

PIAs 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 problems at an early stage, reducing potential distress, subsequent complaints and the associated costs and damage to reputation which might otherwise occur.
It is important to consider whether a PIA is required once the objectives/aims of the project are identified, what is required to successfully meet these and how it is envisaged this will happen, whilst ensuring privacy of personal identifiable information.

Conducting a PIA does not have to be complex or time consuming, if considered at an early stage.

2. Privacy Impact Assessments

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

- identify and manage risks in respect of privacy of personal identifiable information(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 General Data Protection Regulation ((EU) 2016/679). PIAs ensure that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable information.

[1] Under the Data Protection Act, the Information Commissioners Office established a Privacy Impact Assessment Code of Practice, the term Privacy Impact Assessment is used within this document as equivalent to "Data Protection Impact Assessment" as referenced within the General Data Protection Regulation (EU) 2016/679.

[2] Personal Confidential Data has also been referred to as Patient Identifiable Data (PID), Patient Identifiable Information (PII), Confidential Patient Information (CPI) and as personally identifiable.

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

4. Responsibilities

Responsibility for ensuring that a Privacy Impact Assessment is considered and where appropriate, completed, resides with managers leading the introduction of new systems, data sharing or projects. Completion of the Screening Questions on Page 9 evidences that this has been considered.

Line Managers are responsible for ensuring that permanent and temporary staff and contractors are aware of the Privacy Impact Assessment procedure.

There is an expectation that partner organisations/third parties involved in supplying/providing services provide technical information for the Privacy Impact Assessment, as required.

This guidance therefore applies to all staff and all types of information held by the organisation. This procedure should be read in conjunction with the organisation’s IG 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

5. Is a PIA required for every project?

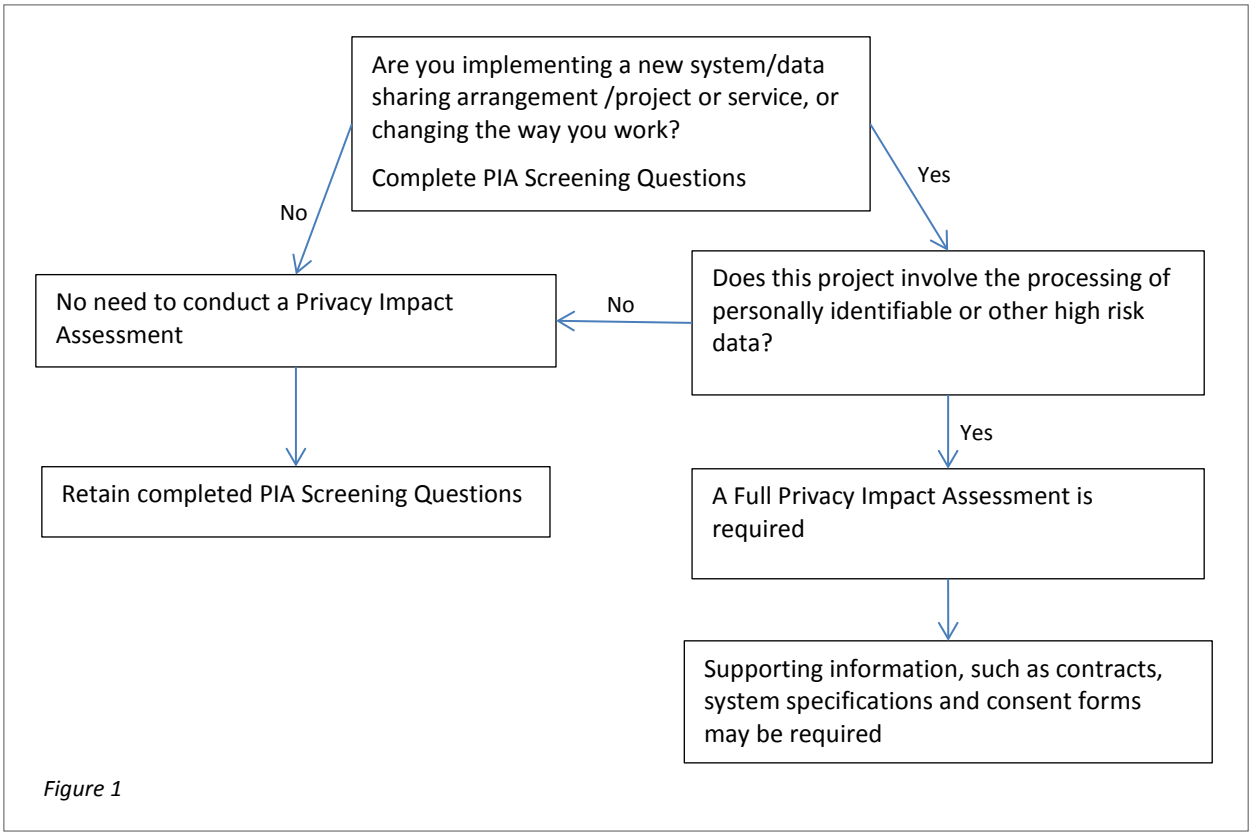

Figure 1

The ICO Code of Practice states that PIAs should be completed where a system/data sharing/project includes the use of personal data, where there is 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 will be reused in a new and 'unexpected' way.

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

Following the review of the Screening Questions it should be determined that a PIA is required. Where it is thought that a PIA is required, The PIA Sections 1-3 should be completed and submitted to the Information Governance Subject Matter Expert for a preliminary review. It is recommended that the IG Subject Matter Expert review is sought

prior to the final PIA being submitted to the Caldicott Guardian (if involving patient identifiable data) or SIRO.

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 Governance 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.

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.

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 processing of identifiable/potentially identifiable data being moved to a new organisation (but with same staff and processes)	☐

Please retain a copy of this questionnaire within your project/system documentation.
Please note that once completed the following sections (1 to 3) should be extracted from the rest of this document prior to being included within the Publication Scheme.

Privacy Impact Assessment (PIA)

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

Section 1: System/Project General Details

System/project/process (referred to thereafter as 'project') title:	Click here to enter text.	
Objective:	Click here to enter text.	
Detail: Why is the new system/change in system required? Is there an approved business case?	Click here to enter text.	
Stakeholders/Relationships/Partners: Please outline the nature of such relationships and the corresponding roles of other organisations.	Click here to enter text.	
Other related projects:	Click here to enter text.	
Project lead:	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	Name:	Click here to enter text.
	Title:	Click here to enter text.
	Department:	Click here to enter text.
	Telephone:	Click here to enter text.

an Information Asset Administrator (IAA) who reports the IAO. IAA's are normally System Managers/Project Leads.	Email	Click here to enter text.

Section 2: Privacy Impact Assessment Key Questions

	Question	Response
Data Items		
1.	**Will the project contain identifiable or Personal Confidential Data (PCD)?** If answered 'No' then a PIA is not normally suggested.	☐ Yes ☐ No If yes, who will this data relate to: ☐ Patient ☐ Staff ☐ Other: Click here to enter text.
2.	**Please state purpose for the processing 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** **Special categories of personal data (sensitive data)**	☐ Name ☐ Address ☐ Post Code ☐ Date of Birth ☐ GP Practice ☐ Date of Death ☐ NHS Number ☐ NI Number ☐ Passport Number ☐ Pseudonymised Data ☐ Online Identifiers (e.g. IP Number, Mobile Device ID) ☐ Health Data ☐ Trade Union membership ☐ Political opinions ☐ Religion ☐ Racial or Ethnic Origin ☐ Sex life and sexual orientation ☐ Biometric Data ☐ Genetic Data ☐ Other:
4.	**What consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of personal and/or sensitive data for this project?**	Click here to enter text.
5.	**How will the data be kept up to date and checked for accuracy and completeness?**	Click here to enter text.
Data processing		
6.	**Will a third party be processing data?**	☐ Yes ☐ No If no, please go to the Confidentiality section.

	Question	Response
7.	**Is the third party contract/supplier of the project registered with the Information Commissioner?** This is required until 25 May 2018.	☐ Yes ☐ No Organisation: Click here to enter text. Data Protection Registration Number: Click here to enter text.
8.	**Has the third party supplier completed and published a satisifactory Information Governance Toolkit submission?**	☐ 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 enclose it with this assessment.
9.	**Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** See CCG Contract and Commissioning Information Governance Assurance checklist.	☐ Yes ☐ No Is the contract based on or utilise the NHS standard contract? ☐ Yes ☐ No
10.	**Will other third parties (not already identified) have access to the data?** 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 how individuals will be informed and kept informed about how their data will be processed.** A copy of the privacy/fair processing notice and/or leaflets must be provided.	Click here to enter text.

	Question	Response
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 If yes, please explain: Click here to enter text.
13.	**Are you relying on individuals (patients/staff) to consent to the processing of personal identifiable or sensitive data?** Please provide copies of any consent documentation that will be used**, including patient information leaflets**	☐ Yes ☐ No If yes, will explicit consent will be sought? ☐ Yes ☐ No 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 proposed processing and sharing/disclosures?**	☐ Yes ☐ No If no, please detail: Click here to enter text.
16.	**What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made?	Click here to enter text.
17.	**Will the processing of data be automated?** Will the proposed processing of data involved automated means of processing to determine an outcome for the individual?	☐ Yes ☐ No ☐ Not applicable If yes, please outline what arrangements would be available to allow the individual access to their data and any ability for the individual to extract such data themselves. Please also detail any profiling that may take place as part through automated processing: Click here to enter text.
18.	**What process is in place for rectifying/blocking data?** What would happen if such a request were made?	Click here to enter text.
Engagement		

	Question	Response
19.	**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		
20.	**Does the project involve any new information sharing between stakeholder organisations?**	☐ Yes ☐ No If yes, please describe: Click here to enter text. **Please provide a data flow diagram showing how identifiable information would flow.**
Data Linkage		
21.	**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 showing how identifiable information would flow and ensure this is added to the CCG Information Asset Register**
Information Security		
22.	**Who will have access to the data within the project?** Please refer to roles/job titles.	Click here to enter text.
23.	**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.

	Question	Response
24.	**Detail where will the data be kept/stored/accessed?** Please outline what data will be stored where.	Click here to enter text.
25.	**Please indicate all methods in which data 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.
26.	**Does the project involve privacy enhancing technologies?** New forms of encryption; 2 factor authentication, pseudonymisation.	☐ Yes ☐ No If yes, please give details: Click here to enter text.
27.	**Is there a documented System Level Security Policy (SLSP) or process for this project?** A SLSP is required for new systems.	☐ Yes ☐ No ☐ Not applicable If yes, please provide a copy.
Privacy and Electronic Communications Regulations		
28.	**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 If no, please explain why consent is not being sought first: Click here to enter text.
Records Management		
29.	**What are the specific retention periods for this data?** Please refer to the Records Management Code of Practice Health and Social Care 2016 and list the retention period for identifiable project datasets.	Click here to enter text.
30.	**Will the data be securely destroyed when it is no longer required?**	☐ Yes ☐ No If no, please detail: Click here to enter text.

	Question	Response
Information Assets and Data Flows		
31.	**Has an Information Asset Owner been identified and does the Information Asset and Data Flow Register require updating?** Please see the Information Asset Register and Data Flow Mapping Form.	☐ Yes ☐ No If yes, include the completed Information Asset Register New Entry Form. Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset? ☐ Yes ☐ No If yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review.
Business Continuity		
32.	**Have the business continuity requirements been considered?**	☐ Yes ☐ No ☐ Business Continuity is not applicable Please explain and either reference how such plans link with the organisational plan or why there are no business continunity considerations that are applicable for this project: Click here to enter text.
Open Data		
33.	**Will identifiable/ potentially identifiable from the project be released as Open Data (placed in to the public domain)?**	☐ Yes ☐ No If yes, please describe: Click here to enter text.
Data Processing Outside of the EEA		
34.	**Will any personal and/or sensitive data be transferredto a country outside the European Economic Area (EEA)?**	☐ Yes ☐ No If yes, which data and to which country? Click here to enter text. If yes, are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country? ☐ Yes ☐ No If yes, who completed who determined this? 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:	☐ The IG review and endorsement by IG Subject Matter Expert is attached.
Date:	Click here to enter text.

Information Governance Approval from the Caldicott Guardian or SIRO

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 Data Protection Act 1998/General Data Protection Regulation ((EU) 2016/679).
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 (applicable up to 25 May 2018)	The DPA 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.
General Data Protection Regulation Privaciples of Lawful Processing of Personal Identifiable Information((EU) 2016/679)	The GDPR requires that data controllers ensure personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
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. Implied consent is unique to the health sector and may be revised under the GDPR.
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.
Special categories of personal data (sensitive data)	This means personal data consisting of information as to the: A. Concerning health, sex life or sexual orientation B. Racial or ethnic origins C. Trade union membership D. Political opinions E. Religious or philosophical beliefs F. Genetic data G. Biometric data H.
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 (EU) 2016/679
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.