NHS
Vale of York
Clinical Commissioning Group

Data Protection Impact Assessment Procedure

Author	eMBED Information Governance Team
Date approved	22 November 2018
Committee	Governance Committee
Version	4.0
Review date	November 2020

Version history

Version	Date	Reviewer	Description	Circulation
0.1	12 September 2014	WSYBCSU	Initial Draft	IG Committee
2	12 August 2015	YHCS	Minor revisions and clarifications added	IG Committee
2.1d	30 September 2016	Embed	Revisions throughout to: Structure Grammar Prompts Language Development of DPIA suite of supporting documents to assist organisations when completing a DPIA.	IG Committee
2.1e	7 November 2016	Embed	Minor revisions to wording for screening contact details.	IG Committee
3	1 December 2017	Embed	Minor corrections and revisions to structure, grammar, terminology. Updated to reference requirements under General Data Protection Regulation.	IG Committee
3.1	1 July 2018	Embed	Further amendments to reflect CCG GDPR structure	IG Committee

Contents

1. Introduction 4
2. Data Protection Impact Assessments 4
3. Purpose of a DPIA 5
4. Responsibilities 5
5. Is a DPIA required for every project? 6
6. When should I start a DPIA? 6
7. Publishing DPIAs 7
Data Protection Impact Assessment (DPIA) Screening Questions 8
Data Protection Impact Assessment (DPIA) 9
Appendix A - Example risks 18
Appendix B – Supporting Documents 19
Appendix C - Glossary 20
Appendix D - Further information 24

1. Introduction

Data Protection Impact Assessments (DPIAs)[1] are required under the General Data Protection Regulation (EU) 2016/679, where health data is being used in a manner that it either is identifiable or there is a risk of an individuals' identity being revealed. A DPIA should also be considered where other personal data, for example data about individual staff, is being used in a way that could poses a high level of risk regarding the privacy of those individuals.

DPIAs aid organisations in determining how a particular project, process or system may affect the privacy of the individual. This procedure consists of DPIA Screening Questions and Data Protection Impact Assessment which are designed to enable an assessment *prior to* new services or new data processing/sharing systems being introduced. A DPIA is not effective when key decisions have already been taken. If an assessment is suggested, it should be seen as dynamic and subject to review with any significant change.

DPIAs identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective DPIA 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 that might otherwise occur.

It is important to consider whether a DPIA is required as soon as the objectives/aims of the project are identified to examine what is required to successfully meet these and how it is envisaged this will happen, whilst ensuring privacy of individuals to which the data relates.

Conducting a DPIA should not be complex or time consuming, if it is given due regard at an early stage.

2. Data Protection Impact Assessments

DPIAs identify privacy risks, foresee problems and bring forward solutions. A successful DPIA will:

- identify and manage risks in respect of privacy of personal 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 D).

DPIAs should demonstrate that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable data.

[1] DPIAs were previously known as Privacy Impact Assessments under the Data Protection Act 1998.

3. Purpose of a DPIA

A DPIA 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 Data Protection Impact Assessment is considered and where appropriate, completed, resides with the manager(s) leading the introduction of new systems, data sharing or projects. Completion of the Screening Questions also serves to evidence that this has been considered.

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

There is an expectation that partner organisations/third parties involved in supplying/providing services contribute the necessary technical information for the Data Protection Impact Assessment.

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 Information Governance (IG) policies:

- Subject Access Request (Access to Health Records) Procedure
- Business Continuity Plan
- Confidentiality and Data Protection Policy
- Email Policy
- Freedom of Information and EIR Policy
- Freedom of Information Procedures
- IG Strategy
- IG Policy and Management Framework
- Incident Reporting Policy
- Information Security Policy
- Interagency Information Sharing Protocol
- Internet and Social Media Policies
- Network Security Policy
- Records Management and Information Lifecycle Policy
- Mobile Working Policy
- Risk Management Policy
- Safe Transfer Guidelines and Procedure

5. Is a DPIA required for every project?

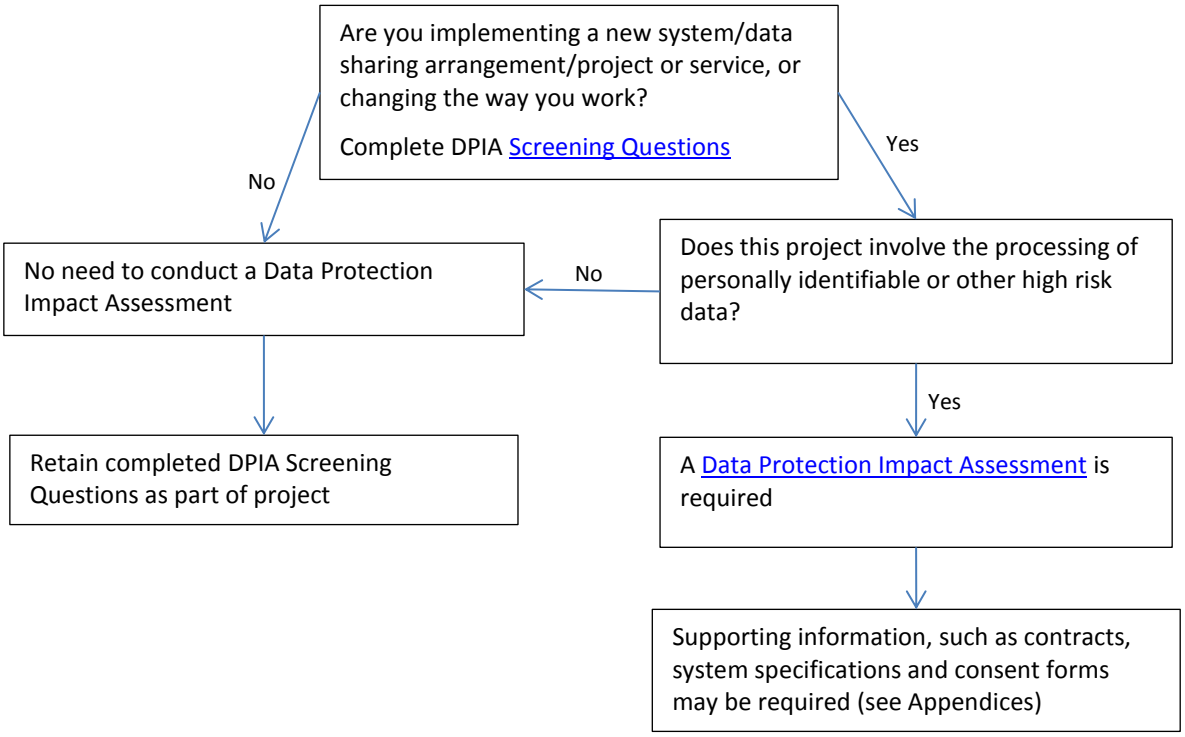

Figure 1

DPIAs 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 data which was originally collected for a limited purpose will be reused in a new and 'unexpected' way.

6. When should I start a DPIA?

DPIAs 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/services
- you have signed contracts/Memorandum of Understanding/agreements

Following the review of the Screening Questions it should be determined that a DPIA is required. Where it is thought that a DPIA is required, The DPIA Sections 1-4 should be completed and submitted to the Information Governance team for a preliminary review. It is recommended that the IG review is sought prior to the final DPIA being submitted to the Data Protection Officer, and Caldicott Guardian (if involving patient identifiable data) or SIRO (if staff data is included). Please

note the controller is required under GDPR to contact the Information Commissioner's Office if processing would result in a high risk in the absence of measures taken to mitigate the risk[2].

7. Publishing DPIAs

All DPIA'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 DPIA'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.

[2] Article 36, General Data Protection Regulation (EU) 2006/679.

Data Protection Impact Assessment (DPIA) Screening Questions

The below screening questions should be used inform whether a DPIA is necessary. This is not an exhaustive list therefore in the event of uncertainty, completion of a DPIA 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.
Date	Click here to enter text.

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

Screening Questions		**Tick**
1	Will the project involve the collection of new identifiable or potentially identifiable data about individuals?	☐
2	Will the project compel individuals to provide data about themselves? i.e. where they will have little awareness or choice.	☐
3	Will identifiable data about individuals be shared with other organisations or people who have not previously had routine access to the data?	☐
4	Are you using data 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 data 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 (or 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 4) should be extracted from the rest of this document prior to being included within the Publication Scheme. The sections should be reviewed before publication to ensure that there is no sensitive data that requires redaction

Data Protection Impact Assessment (DPIA)

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 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.

Section 2: Data Protection Impact Assessment Key Questions

	Question	Response
Data Items		
1.	**Will the project use identifiable or potentially identifiable data in any way?** If answered 'No' then a DPIA 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 the 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 on the CCG or one of its contractors?**	☐ 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?** This was required until 25 May 2018.	☐ Yes ☐ No Organisation: Click here to enter text. Data Protection Registration Number: Click here to enter text.

	Question	Response
8.	**Has the third party supplier completed and published a satisfactory Data Security and Protection Toolkit submission?** Please note that the Data Security and Protection Toolkit replaced the IG Toolkit from 1 April 2018.	☐ Yes ☐ No If yes, please give organisation code and percentage score: Click here to enter text. *IG Toolkit Score:* ☐ Satisfactory ☐ Not satisfactory ☐ Satisfactory with Improvement Plan If satisfactory with an improvement plan, please request a copy of the plan and enclose it with this assessment. If not satisfactory, please explain how the service has been procured: Click here to enter text.
9.	**Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** See 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 notice and/or 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 the data collected limited to a specific set of predefined categories?	☐ Yes ☐ No If yes, please explain: Click here to enter text.

	Question	Response
13.	**Are you relying on individuals (patients/staff) to explicit 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 (Go to next question) How will consent be obtained and by whom? Click here to enter text. Will the consent cover all proposed processing and sharing/disclosures? ☐ Yes ☐ No If no, please detail: Click here to enter text.
14.	**If explicit consent is not being sought, what legal basis enables this data processing?** For more information about conditions for processing, please see the ICO's GDPR website.	Personal data (identifiers and potentially identifiable data): ☐ Relating to a contract: Click here to enter text. ☐ Legal obligation: Click here to enter text. ☐ Vital interests: Click here to enter text. ☐ Public task: Click here to enter text. ☐ Other: Click here to enter text. Special categories of personal data (sensitive data), *if applicable*: ☐ Medical related: Click here to enter text. ☐ Public Health: Click here to enter text. ☐ Employment related: Click here to enter text. ☐ Vital interests: Click here to enter text. ☐ Already public: Click here to enter text. ☐ Legal claim related: Click here to enter text. ☐ Substantial public interest: Click here to enter text. ☐ Other: Click here to enter text.
15.	**Will identifiable data only be handled within the patients' direct care team (in accordance with the Common Law Duty of Confidentiality)?**	☐ Yes ☐ No If no, please detail: Click here to enter text.
16.	**How will consent, non-consent, objections or opt-outs be recorded and respected?**	Click here to enter text.
17.	**What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made?	Click here to enter text.

	Question	Response
18.	**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 are available to enable the individual access and to extract data (in a standard file format). Please also detail any profiling that may take place as part through automated processing: Click here to enter text.
19.	**What process is in place for rectifying/blocking data?** What would happen if such a request were made?	Click here to enter text.
Engagement		
20.	**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		
21.	**Does the project involve any new data sharing between stakeholder organisations?**	☐ Yes ☐ No If yes, please describe: Click here to enter text. Please provide a high level data flow diagram showing how identifiable information would flow.
Data Linkage		
22.	**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 and Data Flow Register (see Information Assets and Data Flows section).
Information Security		
23.	**Who will have access to the data within the project?** Please refer to roles/job titles/organisations.	Click here to enter text.

	Question	Response
24.	**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.
25.	**Where will the data be kept/stored/accessed?** Where applicable, please refer to data flow diagram.	Click here to enter text.
26.	**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 ☐ Software ☐ Mobile app ☐ Other: Click here to enter text.
27.	**Does the project involve privacy enhancing technologies?** *New forms* of encryption, two factor authentication and/or pseudonymisation.	☐ Yes ☐ No If yes, please give details: Click here to enter text.
28.	**Is there a documented System Level Security Policy (SLSP) or process for this project?** A SLSP is required for new *systems* – this is likely to need to be completed by the supplier.	☐ Yes ☐ No ☐ Not applicable If yes, please provide a copy.
Privacy and Electronic Communications Regulations		
29.	**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		
30.	**What are the specific retention periods for this data?** Please refer to the Records Management Code of Practice for Health and Social Care 2016 and list the retention period for identifiable project datasets.	Click here to enter text.

	Question	Response
31.	**Will the data be securely destroyed when it is no longer required?**	☐ Yes ☐ No If no, please detail: Click here to enter text.
Information Assets and Data Flows		
32.	**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		
33.	**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 continuity considerations that are applicable for this project: Click here to enter text.
Open Data		
34.	**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 UK and European Union (EU)		
35.	**Will any personal and/or sensitive data be transferred to a country outside the UK?**	☐ Yes ☐ No If yes, which data and to which country? Click here to enter text.

Section 3: Data Protection Impact Assessment Information Governance Review

Information Governance Review (for completion by IG)				Response (for completion by project lead)	
	Issue	Potential Risk	Recommendation	Agreed Action	Completion (Date and Initials)
1					
2					
3					
4					
5					

For completion by IG:

	Residual Risk	Main Risk Sources	Main Threats	Main Potential Impacts	Main Controls Reducing the Severity and Likelihood	Severity	Likelihood
1							
2							
3							

IG review completed by: Click here to enter text. **Review date:** Click here to enter text.
Date complete and risk assessed: Click here to enter text.

Section 4: Review and Approval

Assessment completed by

Name:	Click here to enter text.
Title:	Click here to enter text.
Date:	Click here to enter text.

Information Governance Approval from the Data Protection Officer *and* Caldicott Guardian or SIRO

Name:	Click here to enter text.
Title:	Click here to enter text.
Approval	☐ The DPO review has been completed and attached.
Date:	Click here to enter text.

Name:	Click here to enter text.
Title:	Click here to enter text.
Approval	☐ The Caldicott Guardian/SIRO 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 data protection 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/General Data Protection Regulation (EU) 2016/679.
ii. Non-compliance with the Common Law Duty of Confidentiality.
iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
iv. Non-compliance with sector specific legislation or standards.
v. Non-compliance with Human Rights Act 1998 and Equality Act 2010.

Appendix B – Supporting Documents

Provider Contract and Commissioning Information Governance Assurance
This guidance should be followed when entering into a contract, which must be present if any personal data is flowing/being transferred/processed:

Contract and Commissioning Inform

Information Asset and Data Flow Register Entry Form and Handbook
Should be completed for any data corresponding to the activity that will be held either by the organisation or on behalf of it (that the organisation would have access to) and any transfers/flows of personal data must be documented:

New entry form for new Information Asse

IAO Handbook v2.0 Sep17 final.pdf

System Level Security Policy Template
Should be completed by the provider/supplier of any system/product where personal data will be stored/flow through:

eMBED System Level Security Policy Toolkit

Data Sharing Agreement Template (Appendix III of the regional Inter-Agency information Sharing Protocol)

Standard Contract Clauses (General Condition 21 of the NHS Standard Contract)
This text covers Patient Confidentiality, Data Protection, Freedom of Information and Transparency. Text must be reviewed to suit individual contracts unless the whole NHS Standard Contract is being used.

Appendix C - Glossary

Item	*Definition*
Anonymised Data	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
Common Law Duty of Confidentiality	This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances: • Where the individual to whom the information relates has consented • Where disclosure is in the overriding public interest; and • Where there is a legal duty to do so, for example a court order • The common law applies to information of both living and deceased patients. The Common Law Duty of Confidentiality persists through the changes to data protection legislation in 2018.
Data Protection Act 2018	The 2018 Act is secondary to the requirements of the GDPR, which means the Act covers national derogations and otherwise supplements the Regulations. The Act specifies the age of 13 years as sufficient to seek consent for the

	processing of personal data and also identified the Information Commissioner's Office as the national supervisory authority.
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. GDPR only recognises explicit consent.
General Data Protection Regulation (EU) 2016/679 Principles of Lawful Processing of Personal Identifiable Information	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 The implementation of the Regulation completed by 25 May 2018.
Information Asset Administrator (IAA)	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
Information Asset Owner (IAO)	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 unique to the health sector and *is no longer recognised* under the GDPR (from 25 May 2018).** 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. GDPR recognises pseudonymised data as personal data with mitigation in place, if implemented correctly, to protect individuals' privacy and confidentiality.
Records	Is a guide to the required standards of practice in the management of

Management: NHS Code of Practice	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 Most of these categories were previously referred to as “sensitive data” under the Data Protection Act 1998.
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 D - Further information

Relevant statutory legislation and law:

Common Law Duty of Confidentiality
Data Protection Act 2018
Freedom of Information Act 2000
General Data Protection Regulation (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
ICO Anonymisation: managing data protection risk code of practice may help identify privacy risks associated with the use of anonymised personal data
ICO Data sharing: code of practice may help to identify privacy risks associated with sharing personal data with other organisations