

Data Privacy Impact Assessment Policy

V6.0

June 2022

Summary

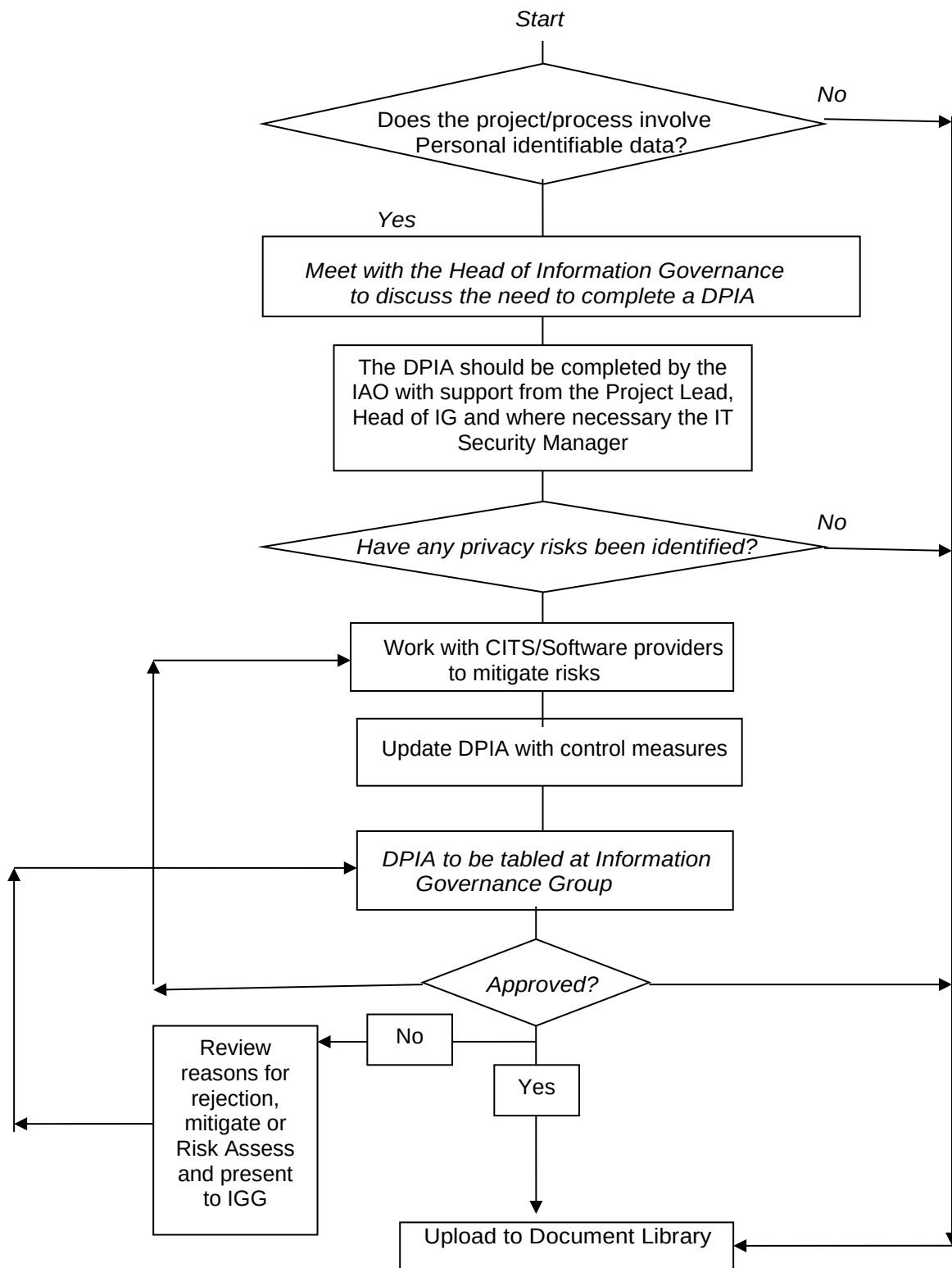


Table of Contents

Summary	2
1. Introduction.....	5
2. Purpose of this Policy/Procedure	5
3. Scope.....	5
4. Definitions / Glossary	5
5. Ownership and Responsibilities	5
5.1. <i>Role of the Chief Executive</i>	5
5.2. <i>Role of the Caldicott Guardian</i>	6
5.3. <i>Role of the Senior Information Risk Owner</i>	6
5.4. <i>Role of the Information Asset Owners</i>	6
5.5. <i>Role of the Project Leads</i>	6
5.6. <i>Role of Managers</i>	6
5.7. <i>Role of IT Security Manager</i>	6
5.8. <i>Role of the Line Managers</i>	6
5.9. <i>Role of the Information Governance Group</i>	6
5.10. <i>Role of Individual Staff</i>	7
6. Standards and Practice	7
6.1. What is privacy?	7
6.2. Privacy risks.....	8
6.3. Data Protection Impact Assessment (DPIA)	8
6.4. The Process.....	9
7. Dissemination and Implementation	10
8. Monitoring compliance and effectiveness	10
9. Updating and Review	11
10. Equality and Diversity	11
The Initial Equality Impact Assessment Screening Form is at Appendix 2.	11
Appendix 1. Governance Information	12
Appendix 2. Equality Impact Assessment	15
Data Privacy Impact Assessment.....	18

Data Protection Act 2018 (General Data Protection Regulation – GDPR) Legislation

The Trust has a duty under the Data Protection Act 2018 and General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed, and documented. We cannot rely on opt out, it must be opt in.

Data Protection Act 2018 and General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and General Data Protection Regulations 2016/679 please see the Information Use Framework Policy or contact the Information Governance Team

Royal Cornwall Hospital Trust rch-tr.infogov@nhs.net

1. Introduction

- 1.1. For many organisations, privacy poses risks which need to be professionally managed in a similar way to other categories of risk. Royal Cornwall Hospitals Trust recognises that handling data is an intrinsic and critical aspect of their business, and that the implementation of projects that handle personal data need to monitor.
- 1.2. It is important to note that any collection, use or disclosure of personal information has the potential to have a risk to personal privacy. Sometimes those risks are not obvious and as a result it can be easy to overlook or not adequately address them.
- 1.3. This version supersedes any previous versions of this document.

2. Purpose of this Policy/Procedure

This policy and attached form are designed to illustrate the approach that the Trust is taking in regard to monitoring and assessing any changes to, or implementation of any new information systems. The careful analysis at the planning stage of intended projects will be enhanced by the implementation of Data Protection Impact Assessment (DPIA) on all new projects.

3. Scope

- 3.1. The term project used in this policy and procedure encompasses any activity that may alter, dispose of or initiate a new system that contains, or potentially contains personal data, whether in an electronic or paper format.
- 3.2. This policy and procedure will apply across the Trust and contracted services where personal data is either managed or processed. All relevant projects must have a DPIA Screening or Assessment completed at an early stage.

4. Definitions / Glossary

- 4.1. DPA18 – Data Protection Act 2018 UK legal implementation of the GDPR
- 4.2. DPIA – Data Protection Impact Assessment (DPIA) process for assessing risk
- 4.3. GDPR – General Data Protection Regulations, European legislation for the protection of personal information.
- 4.4. IGG – Information Governance Group
- 4.5. SIRO – Senior Information Risk Officer. (Person responsible for risk)

5. Ownership and Responsibilities

5.1. *Role of the Chief Executive*

The Chief Executive is responsible for maintaining privacy and confidentiality within the Trust.

5.2. ***Role of the Caldicott Guardian***

The Caldicott Guardian is responsible for protecting the confidentiality of patient information and acts as the conscience of the Trust to ensure

5.3. ***Role of the Senior Information Risk Owner***

The Senior Information Risk Owner and the Head of Information Governance/Data Protection Officer responsible for ensuring IGG review of all Trust DPIA's and ultimate approval.

5.4. ***Role of the Information Asset Owners***

Information Asset Owners are responsible for ensuring that a DPIA conducted whilst given consideration to Access Control, availability, integrity and data quality.

5.5. ***Role of the Project Leads***

All Project Leads (either Business or Project managers) within the Trust are responsible for ensuring that DPIA's are carried out, and presented to the IGG on all new projects.

5.6. ***Role of Managers***

All managers are to be aware of the need for DPIA's for all new projects.

5.7. ***Role of IT Security Manager***

The IT Security Manager is responsible for assessing any IT security needs.

5.8. ***Role of the Line Managers***

Line managers are responsible for:

- Ensuring any new process or system that contains handles or uses personal identifiable data has a DPIA conducted prior to implementation.
- Ensuring any new/changed processes, policies, procedures or office locations (including moves) are assessed using the DPIA to ensure confidential information is secure.

5.9. ***Role of the Information Governance Group***

The Information Governance Group is responsible for:

- Receiving completed DPIA's and recommendations from the Head of Information Governance.
- Approving or seeking further clarification as to issues as required.

5.10. ***Role of Individual Staff***

All staff members are responsible for:

- Ensuring they alert either their line manager or the Head of Information Governance to changes to process where personal identifiable data is used.
- Raise awareness where they think personal identifiable data is at risk.

6. Standards and Practice

6.1. ***What is privacy?***

- 6.1.1. Interpreted most broadly, privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. However, for the purposes of completing a Data Privacy Impact Assessment (DPIA), it is more useful to examine different aspects of privacy. A DPIA could consider:
- 6.1.2. Privacy of personal information is referred to variously as 'data privacy' and 'information privacy'. Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is processed by another party, the individual should be able to exercise a substantial degree of control over that data and its use.
- 6.1.3. Privacy of the person, sometimes referred to as 'bodily privacy', is concerned with the inviolability of the individual's body. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as separate human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.
- 6.1.4. Privacy of personal behaviour relates to the observation of what individuals do and includes such issues as optical surveillance and 'media privacy'. It could relate to matters such as sexual preferences and habits, political or trade union activities and religious practices. But the notion of 'private space' is vital to all aspects of behaviour, is relevant in 'private places' such as the home and toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.

- 6.1.5. Privacy of personal communications could include various means of analysing or recording communications such as mail 'covers', the use of directional microphones and 'bugs' with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third party access to email messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.

6.2. **Privacy risks**

- 6.2.1. The enormous increases in the collection, storage, use and disclosure of personal data, and the imposition of many intrusive technologies, have caused increased concern about individual privacy.

- 6.2.2. Privacy risks fall into two categories.

1. Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.
2. Risks to the organisation as a result of: perceived harm to privacy.
 - A failure to meet public expectations on the protection of personal information;
 - Retrospective imposition of regulatory conditions;
 - The costs of redesigning or delaying a system;
 - The collapse of a project or completed system;
 - Withdrawal of support from key supporting organisations due to perceived privacy harms; and/ or
 - Failure to comply with the law, leading to:
 - Enforcement action; or
 - Compensation claims from individuals.

6.3. **Data Protection Impact Assessment (DPIA)**

- 6.3.1. A DPIA is a systematic process for evaluating a proposal or project in terms of its impact upon privacy. A DPIA can assist in:
- Identify potential issues and concerns on individual or group privacy
 - Examine how detrimental effects may be overcome.
 - Ensure that new projects comply with privacy law and principals.

- Avoiding loss of trust and reputation.
 - Avoiding unnecessary costs and inadequate solutions
- 6.3.2. A DPIA must be seen as a separate process from compliance checking or data protection audit processes. Projects which are already up and running should not be submitted to a DPIA, but to either a compliance check or a data protection audit, whichever is more appropriate.

6.4. The Process

6.4.1. Identifying the need for a DPIA.

The need for a DPIA can be identified as part of an organisation's usual project management process or by using the screening questions in Appendix 3 of this Policy.

6.4.2. Describing the information flows.

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

6.4.3. Identifying the privacy and related risks.

6.4.3.1. Some will be risks to individuals – for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.

6.4.3.2. Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.

6.4.3.3. Legal compliance risks include the Data Protection Act, Privacy and Electronic Communications Regulations, Regulation of Investigatory Powers Act and the Human Rights Act.

6.4.4. Identifying and evaluating privacy solutions.

6.4.4.1. Explain how you could address each risk. Some might be eliminated altogether.

6.4.4.2. Other risks might be reduced. Most projects will require you to accept some level of risk and will have some impact on privacy. Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective

6.4.5. Signing off and recording the DPIA outcomes.

- 6.4.5.1. Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.
- 6.4.5.2. A DPIA report should summarise the process and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate or accept the identified risks.
- 6.4.5.3. Publishing a DPIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

6.4.6. Integrating the DPIA outcomes back into the project plan.

- 6.4.6.1. The DPIA findings and actions should be integrated with the project plan. It might be necessary to return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.
- 6.4.6.2. A DPIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

7. Dissemination and Implementation

- 7.1. This document will be made available on the Trusts Document Library. It will also be highlighted to the Cornwall IT Services management to ensure it is adopted by its Project Managers.
- 7.2. This requirement has been in existence for a number of years, no further training is required, just a reaffirming of its existence and the need for compliance.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	The completion of DPIA's for all known projects
Lead	Head of Information Governance, Project Manager, and Information Asset Owner
Tool	The DPIA Template attached as appendix 3

Information Category	Detail of process and methodology for monitoring compliance
Frequency	Assurances should be sought from the Chief Information Officer, Business & Infrastructure Programme Manager and Head of Information Governance quarterly as to the level of compliance. A DPIA should be completed for all projects where there is a new use of information or where there is a significant change of an existing process. All DPIA's will be tabled at the IGG. These are bi-monthly.
Reporting arrangements	The IGG will receive the DPIA's once approved by the SIRO. The SIRO and Head of Information Governance will make appropriate recommendations. These responsibilities are listed in the duties of the IGG.
Acting on recommendations and Lead(s)	The IGG will require action plans on any recommendations made to DPIA's that do not meet the required standards. The action plan for actions will be determined by the constraints of the delivery of the project.
Change in practice and lessons to be shared	Any changes to the design of the project will be built into the project plan and will be managed by the Project Manager. The Project Manager will be responsible for ensuring the actions are undertaken on an agreed time frame.

9. Updating and Review

- 9.1. This policy should be reviewed every three years. The IGG will be the mechanism for this.
- 9.2. Revisions can be made ahead of the review date when the procedural document requires updating. Where the revisions are significant and the overall policy is changed, the author should ensure the revised document is taken through the standard consultation, approval and dissemination processes.
- 9.3. Where the revisions are minor, e.g., amended job titles or changes in the organisational structure, approval can be sought from the Executive Director responsible for signatory approval, and can be re-published accordingly without having gone through the full consultation and ratification process.
- 9.4. Any revision activity is to be recorded in the Version Control Table as part of the document control process.

10. Equality and Diversity

- 10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the Equality, Diversity & Human Rights Policy or the Equality and Diversity website.

10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	Data Privacy Impact Assessment Policy V6.0
This document replaces (exact title of previous version):	Data Privacy Impact Assessment (DPIA) Policy V5.1
Date Issued/Approved:	14 June 2022
Date Valid From:	June 2022
Date Valid To:	June 2025
Directorate / Department responsible (author/owner):	Mark Scallan – Head of Information Governance
Contact details:	01872 258580
Brief summary of contents:	Data Protection Impact Assessment (DPIA) guide and tool for conducting process. This should be used for all new or significantly changed data collection/processes
Suggested Keywords:	Privacy, By Design, Confidentiality, Risk, Assessment
Target Audience:	RCHT: Yes CFT: No KCCG: No
Executive Director responsible for Policy:	Director of Integrated Governance
Approval route for consultation and ratification:	Information Governance Group
General Manager confirming approval processes:	Mark Scallan, Head of Information Governance
Name of Governance Lead confirming approval by specialty and care group management meetings:	Bernadette George - Director of Integrated Governance
Links to key external standards:	Data Security and Protection Toolkit Data Protection Act 2018 UK General Data Protection Regulation
Related Documents:	Information Use Framework Policy

Information Category	Detailed Information
Training Need Identified?	Yes – Project managers receive annual training in the use of the DPIA.
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet & Intranet
Document Library Folder/Sub Folder:	Health Informatics / Information Governance

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
3 Nov 09	V.1	Initial issue	M Scallan Head of IG.
12 Feb 13	V.2	Updated to POP compliance	M Scallan Head of IG
25 Jan 16	V.3	Changed to show new assessment tool.	M Scallan Head of IG
29 Jun 17	V.4	Changed to reflect changes required for GDPR compliance	M Scallan Head of Information Governance
29 Jan 18	V.4	Changed to reflect changes required for GDPR compliance	M Scallan Head of Information Governance
6 Jun 19	V5	Full Review - Updated assessment form and references to new legislation.	M Scallan Head of Information Governance
14 Jan 20	V5.1	Slight Amendment to the DPIA tool	M Scallan Head of Information Governance
June 2022	V6.0	Full Review – additions made to the DPIA Template to include extra Cyber and Financial fraud questions.	M Scallan Head of Information Governance

All or part of this document can be released under the Freedom of Information Act 2000

This document is to be retained for 10 years from the date of expiry.

This document is only valid on the day of printing

Controlled Document

This document has been created following the Royal Cornwall Hospitals NHS Trust Policy for the Development and Management of Knowledge, Procedural and Web Documents (The Policy on Policies). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Equality Impact Assessment

Section 1: Equality Impact Assessment (EIA) Form

The EIA process allows the Trust to identify where a policy or service may have a negative impact on an individual or particular group of people.

For guidance please refer to the Equality Impact Assessment Policy (available from the document library) or contact the Equality, Diversity & Inclusion Team rcbt.inclusion@nhs.net

Information Category	Detailed Information
Name of the strategy / policy / proposal / service function to be assessed:	Data Privacy Impact Assessment Policy V6.0
Directorate and service area:	Integrated Governance
Is this a new or existing Policy?	Existing
Name of individual completing EIA (Should be completed by an individual with a good understanding of the Service/Policy):	Mark Scallan, Head of Information Governance
Contact details:	01872 258580

Information Category	Detailed Information
(1) Policy Aim - Who is the Policy aimed at? (The Policy is the Strategy, Policy, Proposal or Service Change to be assessed)	To provide a clear process for ensuring the Trust addresses the required confidentiality requirements for projects where there is a likelihood of risk to the privacy and confidentiality of data subjects.
(2) Policy Objectives	To ensure projects consider the requirements of confidentiality and Data Protection.
(3) Policy Intended Outcomes	Projects are implemented safely with the required considerations to confidentiality.
(4) How will you measure each outcome?	Through DPIA completion against the list of approved projects
(5) Who is intended to benefit from the policy?	Trust, Patients, and staff

Information Category	Detailed Information
6a. Who did you consult with? (Please select Yes or No for each category)	1. Workforce: No 2. Patients/ visitors: No 3. Local groups/ system partners: Yes 4. External organisations: No 5. Other: No
6b. Please list the individuals/groups who have been consulted about this policy.	Please record specific names of individuals/ groups: IT Security Information Governance Groupe
6c. What was the outcome of the consultation?	Approved
6d. Have you used any of the following to assist your assessment?	National or local statistics, audits, activity reports, process maps, complaints, staff or patient surveys: No.

7. The Impact

Following consultation with key groups, has a negative impact been identified for any protected characteristic? Please note that a rationale is required for each one.

Where a negative impact is identified without rationale, the key groups will need to be consulted again.

Protected Characteristic	(Yes or No)	Rationale
Age	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Sex (male or female)	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Gender reassignment (Transgender, non-binary, gender fluid etc.)	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Race	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.

Protected Characteristic	(Yes or No)	Rationale
Disability (e.g. physical or cognitive impairment, mental health, long term conditions etc.)	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Religion or belief	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Marriage and civil partnership	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Pregnancy and maternity	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.
Sexual orientation (e.g. gay, straight, bisexual, lesbian etc.)	No	There are no personal aspects to this other than those designed to ensure the confidentiality and security of personal information.

A robust rationale must be in place for all protected characteristics. If a negative impact has been identified, please complete section 2. If no negative impact has been identified and if this is not a major service change, you can end the assessment here.

I am confident that section 2 of this EIA does not need completing as there are no highlighted risks of negative impact occurring because of this policy.

Name of person confirming result of initial impact assessment: Mark Scallan, Head of Information Governance

If a negative impact has been identified above OR this is a major service change, you will need to complete section 2 of the EIA form available here:
[Section 2. Full Equality Analysis](#)

Data Privacy Impact Assessment

Insert name of system

Date:

Section 1: Project/System background (Template is version 9.)

Project/System Name	
---------------------	--

Contacts	Business/Operational lead	CITS lead	Supplier lead (if applicable)	Care Group Information Asset Owner (IAO)
Name				
Role				
Email				
Phone				

What is it that is being planned? Provide a brief description or reference to an Additional Service Request or Project Initiation Document			
Why are we doing it? Summarise the need for change and the benefits it will realise.			
Who are the stakeholders? Please list the RCHT stakeholders and any other organisations that are involved in the process			
Has there been any prior consultation? Detail any previous PIA or DPIA, consultation with Information Governance, Caldicott Guardian, Research/Ethics Groupe etc.			
	Yes	No	
Will the project/system collect/store/process personal identifiable information about patients, staff or other people working for RCHT	☐	☐	If no, a DPIA is not required.
Does the project involve any 3rd party suppliers or partners? If Yes, who are they and what is their role? Please also provide/embed a copy of the contract.	☐	☐	

Section 2: The data

1.	What is the primary reason for processing data? Select one option	Support Direct healthcare		☐	Support management of services and systems	☐
		Manage recruitment		☐	Manage employment	☐
		Clinical audit or service improvement		☐	Manage payments	☐
		Research		☐		
		Yes	No	Notes		
2.	Is there a clear justification for the new data handling, is this clear and is it made known to the data subjects?	☐	☐			
3.	Will the project collect personal information that we don't currently collect?	☐	☐			
4.	Will it use personal information we already collect for the same purpose that we currently use it?	☐	☐			
5.	Will it use personal information we already collect for a different purpose that we currently use it?	☐	☐			
6.	Has an assessment been made that the information collected is the minimum required to meet the aim of the project?	☐	☐			
7.	Can the system be used with anonymised data?	☐	☐			
8.	Can the system be used with anonymised pseudonymised data?	☐	☐			
9.	Extra question – add detail as required.	☐	☐			
10.	Are we making additional uses for identifiers already collected?	☐	☐			
11.	List which Organisations or people who have not previously had routine access to the information?	☐	☐	List Orgs: 1. 2. 3		

12.	Does the project involve you using new technology to access systems/data which do not include the use of entering a digital response e.g. password, pin. For example, • Optical • Finger Print • Facial	☐	☐	Provide detail?
-----	---	--------------------------	--------------------------	-----------------

What data is being collected, shared or used? Please check Yes or No for each data item and where possible provide a reason as to why we need to process this information to achieve the project goal

	Identifying information	Yes	No	Notes
13.	Hospital or NHS number	☐	☐	
14.	Name	☐	☐	
15.	Date of birth	☐	☐	
16.	Address	☐	☐	
17.	Contact details (e.g. address, telephone numbers, email address)	☐	☐	
18.	Gender	☐	☐	
19.	Marital Status	☐	☐	
20.	Picture	☐	☐	
21.	IP Address	☐	☐	

22.	Employee Job Role	☐	☐	
23.	Employee Pay Band	☐	☐	
24.	Bank Details	☐	☐	
25.	Other	Details:		

	Special categories of personal data	Yes	No	Notes	
26.	Data concerning health	☐	☐		
27.	Data concerning sex life or sexual orientation	☐	☐		
28.	Genetic or biometric data	☐	☐		
29	Racial or ethnic origin	☐	☐		
30.	Religious or philosophical beliefs	☐	☐		
31	Approximately how many people will we collect data about?	Less than 1,000		☐	Between 1,000 and 50,000 ☒
		More than 50,000		☐	More than 500,000 ☐
		Yes	No	Notes	
32	Is there an interface to PAS/Maxims/Oceano/ESR to ensure patient demographics are kept up to date? If No, describe how this information is kept accurate and up to date	☐	☐		
33	Where will the data be stored?	Yes	No	Notes	
34	Is the data being stored off site?	☐	☐		
35	Penetration test completion? – executive summary needed for within the last 12 months	Provide summary:			
36	If off site, is it being stored outside the UK?	☐	☐	If not, where is it? EU ☐ Other ☐ Provide details:	
37	Does the data storage facilitate have a Tier rating? i.e., Tier 1 -4	☐	☐		
38	Describe security measures implemented to protect data. E.g., Anti-Virus, Intrusion detection and prevention etc.				
39	Have back up facilities in place been agreed by the IAO?				

40	Account administration: Local (CITS) Supplier	Provide details:		
41	On a server managed by Cornwall IT Services	☐	☐	
42	On a RCHT shared network drive? If Yes, provide location and details of how access will be managed	☐	☐	
43	On The resilient infrastructure (SAN)?	☐	☐	
44	Are the backups managed by CITS?	☐	☐	Details:
45	On the local drive of a RCHT device If Yes, provide location and details of how access will be managed	☐	☐	
46	Backup information: Restore Point Objective/Restore Time Objective	RPO		RTO
47	Have the RPO/RTO been signed off by the IAO?	☐	☐	
48	Will any data be made available to anyone not employed or under contract to RCHT? If Yes, to whom, and why?	☐	☐	
49	Is encryption set to TLS 1.2 or above?	☐	☐	If not to what level?
		Yes	No	
50	Disaster recovery plans	☐	☐	
	Third party assurance			
51	Information Security Management System and/or ISO Certification/CE+	☐	☐	Details:
52	DSPT Compliant	☐	☐	
53	ICO Registration	☐	☐	
	Retention and deletion	Yes	No	Notes

54	The data needs to be retained in accordance with the <u>NHS Records Management Code of Practice</u> . Has provision been made to ensure you are able to accommodate this? If No, describe how the data will be stored	☐	☐	
55	What are the data migration plans, identifying what data is to be retained on legacy system, and for how long. (how will legacy system be maintained and patched to ensure ongoing read only access)	Details:		
56	Is there a process to identify and review data suitable for destruction and/or deletion? If Yes, describe the process and the process to delete or otherwise put the records beyond use	☐	☐	
57	Is there the possibility of the system being exploited for fraud? (Fraud is defined as any dishonest false representation, failure to disclose information or abuse of position) E.g. false time recording (overtime, flexi time, enhanced hours etc), false qualifications/professional registrations, working while sick, claiming additional or fictitious expenses, false charge exemptions, ordering/invoices, mandate fraud, contractor claims, employees not having the correct or legitimate right to work documents, employees having expired right to work documents procuring of goods and services in an non-transparent and dishonest manner, commissioners claiming for services in respect of factious or ghost patients, false identity	☐ ☐ ☐	☐ ☐ ☐	Asset misappropriation Bribery and corruption Financial gain Please provide details:
58	Does the system have logs which can be used to detect fraud? E.g. could the audit logs be used to identify user logging in out of normal hours, detect duplicate activity, unusual changes to data, hacking (such as multiple attempts to log in to an account)?	☐	☐	If yes, please provide detail:
Business Continuity				
59	Has a local Plan been established? IT Provision Service Provision (no IT access)			
60	For how long can the service be delivered in business continuity before patient care is affected through delays or cancellations?			
61	Legacy Systems: Provide details of the business continuity plan if the system becomes unusable or unavailable	Details:		

62	Will the project involve any automated processing to analyse or predict aspects of the person's health or abilities? If Yes, give details.	☐	☐	
63	What procedures in place to ensure that all staff with access to the information have adequate training?			
64	Describe what measures and procedures will be in place to ensure access is restricted on a need to know basis			
65	For electronic records we must be able to trace activity to users. Does the system provide an audit of who has accessed a record?	☐	☐	
66	Describe the process for requesting/producing user activity reports, and attach/embed an example			
67	Will the system require live data to be recorded within the User Acceptance Testing environment?	☐	☐	
68	What data will be Used to train users?	Details:		• Live • Dummy
	Data Connectivity			
69	Network Diagram showing info flows between organisations/data centres/systems	Provide copy		
70	Data Flows – describe what data will be shared and with whom, also any links to other IT Systems – e.g., PAS			

Section 4: Rights of data subjects

71	Individuals need to be told how their information is processed. Is this covered by an existing fair processing information or leaflet? If Yes, provide details. If No, describe how you will inform individuals	☐	☐	
72	Describe the process for making changes to the records of data subjects? E.g. to correct errors, record data subject comments.			
73	Describe the process for extracting data to make disclosures of data subject records from the system.			

Section 5: Legal basis for processing

74	What is the legal basis for processing the information?	Yes	No	Notes -select one
	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested the controller	☐	☐	(will be appropriate choice for healthcare provision)
	Processing is necessary for the performance of a contract	☐	☐	
	Processing is necessary for compliance with a legal obligation to which the controller is subject;	☐	☐	
	Processing is necessary in order to protect the vital interests of the data subject	☐	☐	
	<i>Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party NB. Not for public bodies.</i>	☐	☐	
	Explicit consent If yes, describe how consent will be sought and recorded and attach copies of any consent forms. Individuals must be able to withdraw consent for processing, so describe how they will be able to do so.	☐	☐	
75	What is the legal basis for processing Special Category Data?			Select one.
	the data subject has given explicit consent to the processing of those personal data for one or more specified purposes	☐	☐	
	is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment and social protection law (Safeguarding)	☐	☐	

	Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	☐	☐	
	Processing is carried out in the course of its legitimate activities with appropriate safeguards	☐	☐	
	Processing relates to personal data which are manifestly made public by the data subject	☐	☐	
	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity	☐	☐	
	Processing is necessary for reasons of substantial public interest,	☐	☐	
	Medical diagnosis, the provision of health or social care or treatment or the management of health or social care system	☐	☐	
	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices	☐	☐	(will be appropriate choice for healthcare provision)
	Scientific or historical research purposes or statistical purposes	☐	☐	

Section 6 – Locality changes - Delete section as necessary

76	DPIA to manage change of locality	
77	Is the area going to have personal or sensitive information?	Yes ☐ No ☐
78	Is the new locality on site?	Yes ☐ No ☐

79	If not on site, where is the new locality?	Notes:
80	What contract do we have in place to cover confidentiality/data protection?	Notes:

81	Has a site visit been held?	Yes ☐ No ☐			
82	Results of Site Visit	Notes:			
83	Are there any security measures in place?	Keypad ☐	Swipe card ☐	Lock ☐	Other (specify)
84	Is the area alarmed?	Yes ☐ No ☐			
85	Is there CCTV?	Yes ☐ No ☐			
86	Is it a public access area?	Yes ☐ No ☐			
87	How is the identifiable data being transferred?	Internal Porters ☐			External Removals ☐

Section 7 – Privacy issues/risks identified

Ref.	Risk	Consequence(s)	Risk rating now			Mitigation/Recommended Actions	Risk rating after mitigation			Status
			Likelihood	Consequence	Risk score		Likelihood	Consequence	Risk score	
PR01	none									Open
PR02										Open
PR03										Open
PR04										Open

Section 7 – Approval and recommendations [TO BE ACTIONED BY THE INFORMATION GOVERNANCE TEAM]

This DPIA is...			
APPROVED	☐		
CONDITIONALLY APPROVED (PENDING THE COMPLETION OF THE FOLLOWING ACTIONS)	☐	Not applicable	
REJECTED (FOR THE FOLLOWING REASONS)	☐	Not applicable	
Caldicott Guardian/SIRO name/signature			Date

Final Check List: Have we considered?

- ☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- ☐ We make data protection an essential component of the core functionality of our processing systems and services.
- ☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- ☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- ☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- ☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- ☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- ☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- ☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- ☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- ☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- ☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.