Data Protection Impact Assessment

Contents

Introduction

Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK General Data Protection Regulation's fundamental principles and requirements, and forms part of the focus on accountability.

A Data Protection Impact Assessment (DPIA) is a tool that we use to identify and reduce the data protection risks of our processing activities. They can also help us to design more efficient and effective processes for handling personal data.

The UK General Data Protection Regulation requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.

In essence, this means we have to integrate or 'bake in' data protection into our processing activities and business practices, from the design stage right through the lifecycle. This concept is not new and **is now a legal requirement**.

When and who should complete a DPIA?

- A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed. **No commitments to, or installation of systems, should take place before the DPIA has been signed off.**

- Information Assets Owners (IAO) and Information Assets Administrators (IAA) **must** complete the DPIA.

- Relevant stakeholders (internal and external suppliers) should be consulted throughout the DPIA process.

Who do I send the completed DPIA to for review?

- Information Governance Team sfh-tr.information.governance@nhs.net.

What if I need help?

- Please contact the Information Governance Team sfh-tr.information.governance@nhs.net or SFHT Phonebook (nnotts.nhs.uk)

IMPORTANT – PLEASE COMPLETE ALL QUESTIONS. IF YOU THINK A QUESTION DOES NOT APPLY INSERT N/A AND EXPLAIN WHY.

Project title:	
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	
Information Asset Owner (name and job title)	`
Information Asset Administrator (name and job title)	

Step 1 – What is the aim of the project being undertaken

Q1	**Project description: Describe in sufficient detail for the project to be understood**	

Q2	**Why are we doing it?** Summarise why there is a need for implementation or change and the benefits it will realise.	

Q3	**What is the nature of your relationship with the data subject (patient, staff) whose data will be used?** For example, do you provide direct care to the data subjects, are they your patients?	

Q4	**Individuals need to be told how their information is processed.**	
	Have you consulted the data subject or their representative about using this data? If not, please explain why you haven't consulted them?	
	Please provide details and an example of how this consent (if appropriate to rely on consent as a legal basis) to processing of their data was given? (Preferably embed document)	
	What information will you give individuals informing them of what you are doing with their data? ie this is consent to the processing of their personal data, not consent to treatment	
	Is this information covered by our existing fair processing information or leaflet? If Yes, provide details. If No, please provide text to be added to our fair processing information. Patient[1] Staff[2]	
	Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?	

Q5	**Has an assessment been made that the information collected is the minimum required to meet the aim of the project?**	
	Use of data should not be the first resort if the objective can be achieved without its use. You must justify why the use of all the data is necessary and proportionate. For example, do	

[1] https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/

[2] https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/

	you need to use all the fields, can you not achieve the same objective with fewer data fields and/or a smaller data set?	
	Has consideration been given to how the same objective or outcome may be achieved without using this data or using less data or employing a different method - explain in full?	

Step 2: What type of data is being processed?

Q6	**Fully describe ALL the data that will be used and justify why they are needed.**	
	Data item ie MRI images, patient, name, address, IP address, NHS/D number	**Why is it necessary?**

Q7	**Will you use special categories of personal data?**	
	political opinions	□
	racial or ethnic origin	□
	religious or philosophical beliefs	□
	trade-union membership	□
	genetic data	□
	biometric data for the purpose of uniquely identifying a natural person	□
	data concerning health	□
	data concerning a natural person's sex life or sexual orientation	□

Q8	**Approximately how many individuals will be in the dataset?**	
	<11 individuals	□
	11 – 50 individuals	□
	51 – 100 individuals	□
	101 – 300 individuals	□
	301 – 500 individuals	□
	501 - 1,000 individuals	□
	1,001 - 5,000 individuals	□
	5,001 - 10,000 individuals	□
	10,001 - 100,000 individuals	□
	100,001 or more individuals	□

Q9	**How large and expansive are the records sets being used, what will it consist of?**

Q10	**What geographical area will the data be drawn from or cover?** For example, Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients ?	

Q11	**What is the source of this data?**	
	If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for? How will this data be accessed?	
	If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?	

Q12	**How will this data be used?**	
	Will this data be used or combined with other data sets, if so what are these other data sets?	
	What will this data show you that is relevant to the project aim and purpose?	
	Describe the access controls in place. Will the supplier also have access to the data?	
	Complete the Account Management and Access Standard Operating Procedure[3]	Embed the completed procedure

Q13	**Describe proportionality measures**	
	Explain how the processing achieves your purpose?	

[3] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618

	Is there another way to achieve the same outcome, give details of alternatives you have rejected and provide the reasons why?		
	Please explain why a smaller amount of data cannot be used.		
	Does the National Data Opt-Out apply (allows patients to opt out of their confidential patient information being used for research and planning)?	Yes	No
		□	□

Q14	**What is the duration of this processing?** Is this one off processing or will it continue for a specified period?

Q15	**How long will the data be kept and how will it be deleted?**	
	NHS data needs to be retained in accordance with the Records Management Code of Practice[4]. You can check the schedule here[5]. Has provision been made to ensure you are able to accommodate this? If No, describe how the data will be managed.	
	If data is being processed by a third party, how will we ensure data is deleted when required? Appropriate evidence would be an embedded copy of the contract or agreement containing this detail	
	What will happen to the data at the end of the project/activity or end of contract with a third party? Will it be	

[4] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647

[5] https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule

	returned or deleted and how will this be done? Most contracts specify what happens to data at the end of contract. If this is not subject to contract, how will you ensure the data held by any third party is deleted? Embed extract of contract as necessary with highlighted sections.	

Q16	**Has the personal/special categories of data been minimised?**	
	Please explain why a smaller amount of data cannot be used and explain why all the data fields are necessary to achieve the objective. You are required to minimise the amount and level detail of any data set. For example, dates of birth should not be used where age would provide sufficient information to achieve the project aim.	
	How will you prevent function creep?	
	How will you ensure high standards of data quality?	

Q17	Is the data anonymised or pseudonymised in any way?	Anonymised	Pseudonymised
		□	□
	If the data is pseudonymised please describe how this has been done and the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust.		
	If the data is pseudonymised describe how the data will be transferred ie using HL7. ie Data will be sent using HL7. SSL (Security Socket Layer) and HTTPS (Hypertext Transfer		

	Protocol over Secure Socket Layer) are used in the encrypted transmission of data.	
	Have you considered whether using anonymised/pseudonymised data is a suitable alternative, please explain how this has been considered and why it is not suitable?	
	What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?	

Step 3 – Data security

Q18	**Where will the data be stored?**			
	Will the data be stored on our servers or servers/cloud external to the Trust?			
	Internal	External	Server	Cloud*
	□	□	□	□
	If external, where will it be stored, will this be the UK, EU/EEA or elsewhere? Provide the location/country ie London, England			
	If the data is processed outside of the EU/EEA, what safeguards will be in place?			
	If a supplier is used they must complete the supplier assurance framework below Supplier Assurance Framework TEMPLATE		Insert completed supplier assurance framework or state N/A if a supplier is not used	
	Will the storage be controlled by another party (not the supplier) such as a product/ platform supplier ie AWS, Google, Microsoft? Provide details			
	If the data is stored on the cloud the following assessment must be completed by the supplier Cloud Assessment.xlsx		Insert completed cloud assessment or state N/A if the data is not stored in the cloud	
	If the data storage or processing is being done by a supplier, what certifications do they hold? When were they, and the proposed storage mechanism, subjected to an external penetration test and is a report available? (Please embed any documentary evidence)			
		Certificate	**External Penetration Test**	**External Penetration Test Report**

			undertaken (date)	
	Cyber Essentials +/ Cyber Assessment Framework (CAF)			
	ISO 15489 Records Management			
	ISO 27001 Information Security Standards			
	ISO/IEC 27701:2019 Ext to 27001/27002			
	ISO 27017 Cloud Services			
	ISO 27018 PII in public clouds			
	Digital Technology Assessment Criteria for Health and Social Care (DTAC)			
	ISO 9001 Quality Management Systems			
	Other, please specify			
	If a supplier is used are they registered with the ICO. Check the register[6] and provide the certificate number	Yes	No	
		□	□	
		Registration reference: Z		
	If a supplier is used, have they completed the Data Security and Protection Toolkit, search the register here[7]	Yes	No	N/A
		□	□	□
	If yes, complete the following	Organisation code	Status	Date Published
			Choose an item.	

[6] https://ico.org.uk/ESDWebPages/Search
[7] https://www.dsptoolkit.nhs.uk/OrganisationSearch

Q19	**How will this data be secured during storage and when being moved?**			
	Will it be encrypted when stored and/or moved, if so what type of encryption will be employed?			
	Will it be on a server protected by firewall and network intrusion detection?			
	What technical controls are in place to prevent hacking of the data by unauthorised persons?			
	When being moved will it be secured through encrypted file transfer, secure transmission through SLL/TLS/SHS, please explain the specific technical standards that will apply?			
	Do you have a business continuity plan for the information?			
	What types of backups are undertaken i.e. full, differential or incremental?	Full	Differential	Incremental
		□	□	□

Q20	**Who will have access to this data and how will this access be controlled?**		
	Will the data be kept on a system that is password controlled, what is the password length and how often does it have to be changed? Who will administer these access controls?		
	Is there an ability to audit access to the information? Can the supplier audit our data?		
	What other security measures are in place, such as physical security, smartcard, Active Directory, multiple factor authentication?		
	Is training available to staff for the new system?	Yes	No
		□	□

Q21	**If you are using devices such as laptops to access data, how are these secured and managed?**

Q22	**Is this data an attractive target for criminals and hackers; does it contain information that may be used for identity/financial fraud or reveal a person possibly being vulnerable to exploitation?**	
	Yes □ Rate its attractiveness from 0 to 10 below. https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime Choose an item. If this is a risk describe how you will manage it in stage 8.	No □

Step 4 – Data use and sharing

Q23	**Will this data be shared with anyone else?**	
	If yes, explain who these other parties are and why the data is being shared?	
	What is the statutory reason for this sharing? ie direct care	

Q24	**Are other people processing this data?**	
	If a third party such as a company is storing or otherwise managing or using our data, please explain what they doing and why they are doing it?	
	If we are using a third party product that requires maintenance where they access our networks, explain how this will be managed (will they remotely connect, how will this access be managed).	
	Is there a process in place to remove personal data if data subject refuses/removes consent? ie The right to restrict processing/the right to object - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis.	
	Are arrangements in place for recognising and responding to requests for access to personal data?	The Trust has a policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk)

Q25	**Describe the data flows**	
	Please complete the data flow template below to detail how the data is collected, moved and used?	Embed data flow here

	New Flow Map UPDATED.xlsm	
	Are there security or data protection concerns in any of the data flow stages you identify? If so, please indicate where and what steps you taking to reduce these risk?	

Step 5 – Processing by or with a supplier/third party

Q26	**If you are using a supplier or organisation to process, store or otherwise interact with this data, if not answer N/A**	
	What is the arrangement between the Trust and the supplier/third party concerned?	
	What activities will the supplier/third party carry out i.e. storage, transport, processing of data on their platform	
Q27	What steps or measures will you put in place to manage these risks? What measures will you take to ensure processors comply? PLEASE ATTACH COPIES/ RELEVANT SECTIONS OF ANY CONTRACT/ AGREEMENT.	

Step 6 – Consultation

Q28	**Consider how to consult with those who have an interest in this project**	
	Describe when and how you will seek individuals’ views or justify why it’s not appropriate to do so. ie do we need wider public engagement.	The DPIA will be forwarded to the Information Governance Working Group for wider stakeholder engagement.
	Who else do you need to involve within the Trust? ie Digital Innovations Approval Group (DIAG).	
	Do you need to ask the data processors (supplier) to assist?	
	Do you plan to consult information security experts, or any other experts?	

Step 7 – Lawful basis

Q29	**What is your lawful basis for processing personal data? Select all that apply**	
	a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. **Please note, do not use this if it is for direct care, (e) maybe more appropriate**	□
	b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	□
	c) processing is necessary for compliance with a legal obligation to which the controller is subject	□
	d) processing is necessary in order to protect the vital interests of the data subject or of another natural person	□
	e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	□

Q30	**What is your lawful basis for processing special categories of personal data? Select all that apply**	
	a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. **Please note, do not use this if it is for direct care, (h) and/or (i) maybe more appropriate**	□
	b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment	□
	c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	□
	e) processing relates to personal data which are manifestly made public by the data subject	□
	h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	□

	i) processing is necessary for reasons of substantial public interest, ie public health, such as protecting against serious cross-border threats to health	□
	j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose	□

Stage 8 – Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

Completed by:	Role:	Date completed:

Guidance notes:

Confidentiality - Are there any risks to the confidentiality of personal data? Do staff have a legitimate relationship in order to process personal data? Is personal data disclosed to people who do not require it?

Integrity - Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.

Availability - System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

Examples of risks that are common in projects is included below. Please amend/delete as necessary.

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Loss of system access due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be enforcement action and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place Business continuity plan in place Regular updates from supplier to advise users of any planned updates and a process is in place to contact all main users for support during any unplanned downtime	2	2	4		2	2	4	
Loss of system data due to connection failure or server failure by third party supplier.	Full system back-up processes and ISO 27001, 27017 and 27018 accreditation in place Business continuity plan in place	2	2	4		2	2	4	

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
This could result in the service being disrupted or unavailable. The consequences of this could be enforcement action and reputational damage to the Trust									
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the xx	2	2	4		2	1	**2**	XX will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Access is managed within the XX team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place.	2	2	4	There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records. The system will only allow one generic account and individual users cannot be tracked or audited	2	2	**4**	
Issue with interface between system and system causing delays in clearance data being updated on system	Regular updates from system team to advise users of any planned updates and process to contact all main users for support during any unplanned downtime – during any extended downtime xx team would manually advise xx of status	2	2	4		2	2	**4**	

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Data is lost during the migration from old system to new system requiring xx team to access paper records for historical information	Following migration of data the xx team will conduct a review of a selection of records to ensure the integrity of data transferred Work would need to be undertaken with supplier to establish why the data did not migrate and what actions can be taken to rectify								
Adequate data processing agreements with relevant data processors	A contract and data processing agreement between XX and XX developed. Separate processing agreements where necessary will be in place with additional providers of data to XX.	3	1	3					

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Personal data not being encrypted both/either in transit or at rest	Web-upload technology which automatically compresses all images/data before transit and transmits the above over HTTPS/TLS1.3 encrypted connection	3	1	3					

Risk Scoring Matrix.pdf

Step 8 – Legal compliance

To be amended by Information Governance from the responses provided in the previous stages.

UK General Data Protection Regulation 2018	Compliance
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest, and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

	• If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.
Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes. • We periodically review the data we hold, and delete anything we don’t need.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual’s right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to three Inquiries including the Goddard Inquiry, no destruction or deletion of patient records is to take place until further notice. • We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. • When deciding what measures to implement, we take account of the state of the art and costs of implementation • We have an information security policy and take steps to make sure the policy is implemented. • When deciding what measures to implement, we take account of the state of the art and costs of implementation • We make sure that we regularly review our information security policies and measures and, where necessary, improve them. • We have assessed what we need to do by considering the security outcomes we want to achieve. • We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. • We use encryption and/or pseudonymisation where it is appropriate to do so. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.

Principle 7 – Accountability principle	• We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation. • We keep evidence of the steps we take to comply with the UK GDPR. • We put in place appropriate technical and organisational measures, such as: ☐ adopting and implementing data protection policies (where proportionate); ☐ taking a ‘data protection by design and default’ approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations; ☐ putting written contracts in place with organisations that process personal data on our behalf; ☐ maintaining documentation of our processing activities; ☐ implementing appropriate security measures; ☐ recording and, where necessary, reporting personal data breaches; ☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests; ☐ appointed a data protection officer; and ☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible). ☐ We review and update our accountability measures at appropriate intervals.

Step 9 - Assessment Summary

To be completed by Information Governance.

Outcome of Data Protection Impact Assessment	
Project is not recommended to proceed, as significant risks have been identified.	☐
Project to proceed once identified risks have been mitigated as agreed.	☐
Project has met required legislative compliance and poses no significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks	
Legislative Compliance:	**Suggested text, remove, amend as necessary.** Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity) Article 9(2)(i) allows processing for “ensuring high standards of quality and safety of health care.” – which would cover research, audit, service improvement and addressing public health/inequalities
Summary of Risks	**Suggested text, remove, amend as necessary.** Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.
Identified risks	
The risk	**Mitigation**
Loss of system access	Full system back-up process in place

Loss of system data	Full system back-up process in place
Data is accessed inappropriately	individual username and passwords are provided. There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records
Issue with interface between system and system causing delays in clearance data being updated on system	
Data is lost during the migration from old system to new system requiring xx team to access paper records for historical information	
Adequate data processing agreements with relevant data processors	
Personal data not being encrypted both/either in transit or at rest	

Step 10 - Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	**Recommendations**	**Agreed deadline for action**
Information Asset Administrators to ensure XX is added to the information asset register and data flows are mapped and recorded	IAO/IAA	
Ensure business continuity plans are in place	IAO/IAA	
Account management Standard Operating Procedure generated and implemented, routine audit to take place	IAO/IAA	

Step 11 - Project signoff

	Name	Job Title	Date
Information Asset Owner*		Divisional General Manager	
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	
Caldicott Guardian	David Selwyn	Medical Director	
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	
Patient safety[8]			

The Data Protection Impact Assessment must be reviewed and approved by the Information Asset Owner, Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian.   Approval does not close the data protection risks related to this project.

*It is important that the risks and the original scope of the project are reviewed on a regular basis to ensure any new confidentiality, integrity or availability risks are identified, documented, and mitigated wherever possible. All amendments must be approved following the approvals process.

[8] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital