Criteria for DPIA

This section should be used when conducting a DPIA.

The evaluation process involves answering a set of questions about characteristics of a project / service or an I.T system. These are factors that tend to give cause to concern among at least some parts of the general public, and accordingly may be judged to represent project risk factors. Please add further information in the comments section as required to help identify any risks or issues. Actions should then be developed and assigned to an owner to be completed prior to the system / service being accredited / approved.

Questions	Yes/No	Comments must be included to support your answer	Action	Owner
1. Project Information				
a. Refer to Information Security Tab				
b. Who is the identified IAO?	Yes	Accountable Officer, Lincolnshire East CCG		
c. Who is the IAA?	No	not applicable		
d. What type of data will be collected?	No	view only		
e. Where is the data held?	Yes	In the UK		
f. Is the information being used for a different purpose than it was originally collected for?	No			
g. Are we a data processor or data controller in terms of this process?	Yes	Data Processor		
h. Are other organisations / individuals involved in processing the data and are they registered with the information commissioners office?	No			
i. Data security protection toolkit version and score for all third parties are known/recorded?	Yes	This is publicly available information		
j. Is there a sharing agreement in place?	Yes	ISA in place and signed by all organisations using the Care Portal		
k. Have data flows been identified?	Yes	Architecture diagram is available if required.		
l. Is there a contract in place and is it GDPR compliant?	Yes	Confirmed		
m. Does the work involved employing contractors external to the organisation?	Yes			
n. Who will have access to the information?	Yes	Each organisation will have assigned users		
o. Will information be sent off site and how will this transfer of information be secured (e.g. encryption)?	No			
p. Is any data been transferred/processed outside of the EU?	No			
q. How long will information be retained by each processor and what are the arrangements for archival process and destruction?	Yes	Responsibility of each organisation with system connected		
r. How are we letting individuals know about this new process/system?	Yes	Comms - leaflets, posters, website, privacy notice, press		
s. Does the privacy notice need to been updated?	No	Notice is on the Lincolnshire STP website		
2. Technology & Privacy by Design				
a. Refer to Information Security Tab				
2. Justification				
a. Is there a legal basis as part of sharing information for this project, if yes add this to the comments section?	Yes	Legal basis set out in Care Portal GDPR compliance document		
b. If the system / project / process relying on consent? And if yes is the consent GDPR compliant?	Yes	Implied consent - further detail in Care Portal GDPR compliance document		
3. Identity				
a. Does the project involve an additional use of an existing identifier?	No			
b. Does the project involve use of a new identifier for multiple purposes?	No			
c. Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?	No			
4. Data Subject Rights				
Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?	No			
a. Can the data subject obtain a copy of their information?	Yes	via the relevant organisation		
b. Does the system/process support the right to rectification?	Yes	via the relevant organisation		
c. Does the system allow the data to be erased?	Yes	via the relevant organisation		
d. does the system / service support the right to prevent processing?	Yes	Individuals can opt out		
e. will the system have any automated system processing including profiling?	No			
f. Can the system / process meet the right to data portability?	No			
g.Can the system / process support the right to object to processing?	Yes	Individuals can opt out		
h. Does the system/process involve research?	No			
i. Can the data be audited (including view only)?	Yes	Audit reporting area available to IG colleagues		
j. Will the project involve the collection of genetic data?	No			
k. Will the project involve the collection/use of biometric data?	No			
5. Data Handling				
a. Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?	No			
b. Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?	No			
c. Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?	No			
d. Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?	No			
e. Does the project involve new or changed data retention arrangements that may be unclear or extensive?	No			
f. Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?	No			
6. Exemptions				
a. Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?	No			
7. Business Continuity				
a. Refer to Information Security Tab				
8. Records Management				
a. Is there a Records Management Plan in-place when decommissioning the contract to ensure existing records are transferred or accessed as appropriate. If nothing in place – Risk to be noted.	Yes	Each contributing organisation's responsibility		

Information Security Risk Assessment

Questions	Yes/No	Comments must be included to support your answer	Action	Owner
1. Project Information				
a. Does the system involve new links with personal data held in other systems, or have existing links been significantly changed?	Yes	The Linconshire Care Portal provides a single integrated view of an individuals' health and care record which appropriate health and care workers will be able to access. It does not create a new record but pulls all patient information from the health and care systems connected to the Portal to provide a dashboard view.		
b. If the system is managed where will the data reside, will it be in the EU? Will the data be stored in the Cloud?	No	not applicable - see above.		
c. If the system is managed by a third party, does the system supplier use any external 3rd party companies / hosting services?	No	The Care Portal is hosted at Lincoln County Hospital, managed by ULHT IT Team. Supplier provide system maintenance & support.		
d. Does the project involve new linkage of personal data with data in other collections/system, or significant change in data linkages? E.g. is there a need to interface the new system with a current system?	Yes	The Care Portal connects to organisation's electronic systems to surface items from a patient's health and care record.		
2. Information Security Policy				
a. Does the system have a specific system security policy?	Yes			
3. Organisation of information security				
a. Has an Information Asset Owner (IAO) has been identified?	Yes	Accountable Officer, LECCG		
b. Has an IAO group ,has been identified / is one being set up?	Yes	Care Portal IG Group and STP Data Security and Protection Group		
4. Asset Management				
a. Has the System been registered on the Trust Information Asset Resister	Yes	Each organisation with a connected system should have it on their asset register		
5. Information Classification				
a. The system has been identified as a confidential system and all appropriate measures will be taken to protect output by marking documents and if necessary screen displays	Yes	There is protective labelling on documents		
6. Access Control				
Users access is based on the following statement - 'Only authorised individuals, who have a genuine need to access the information (held on/or processed by a system) to enable them to perform their duties, are to be granted access'	Yes	Care Portal has Role Based Access Controls and supports concept of Legitimate Relationships.		
Access Control Model adopted including:				
a) Identification and approval of users roles - Sponsorship	Yes	Manager approval required		
b) Access levels based on Role Based Access Control (RBAC)	Yes	Access cannot be given until an RBAC role is assigned to the user		
c) Access levels documented - Role map produced	Yes	the data and functionality assigned to each role is documented		
d) Access levels recorded against individuals given access	Yes	each user is assigned a role		
e) System training identified and completed before access is granted	Yes	e-learning		
f) Access is granted on the basis of individual approval or position based model i.e. One or both of the following role allocation methods is used, access roles are created and issued based on: 1. an agreed request process - individual sponsorship, 2. or by Trust policy i.e. base line requirement /Access control Position - Trust sponsorship	Yes	Individual sponsorship		
g) One or more of the following user authentication methods is used: NHS CRS smartcard, or other two factor authentication. Username and Password	Yes	linked to Active Directory logins for NHS orgs, otherwise username & password, also smartcard access available.		
h) Access is removed in a timely manner when user no longer requires the access	Yes	account deactiviation is linked to Active Directory & Smartcards, BAU processes for non AD users developed as part of onboarding process.		
i) Individual accounts to be created (no generic accounts)	Yes	Each user has their own care portal account		
7. Password Management				
Password management enforced including:				
a) A minimum length of 8 characters	Yes			
b) Initial password to be of sufficient strength to protect the system - inappropriate or obvious passwords are not being used	Yes			
c) Users to be forced by the system or required by policy to change their initial passwords on first login	Yes	This only applies to non Active Directory accounts.		
d) Password are a combination of letters and numbers/special characters	No			
e) User are forced by the system to change passwords every 30 days	Yes			
8. Asset & Data Security				
a. Secure approved storage for servers - i.e. dedicated server rooms	Yes			
b. Is there fail over servers/back ups and where do they reside? Are they EU based?	Yes			
c. All computer screens are positioned in controlled areas or away form public access / view?	No	responsibility of each org		
d. All mobile devices or exposed desktops used are encrypted?	Yes			
e. All remote access by users is secure?	Yes			
f. System has audit trail facilities (including view only)?	Yes			
9. Operation procedures				
a. Documented operational procedures will be developed?	Yes			
b. Configuration Control Change management procedures will be adopted?	Yes			
c. There will be a separate test and development system?	Yes			
10. Third Party service delivery management				
a. There are no un approved connectivity to other systems or third party access - 'back doors' ?	No			
b. Any third party processes are based on formal NHS/Government standard contract arrangements which include GDPR approved IG clauses?	Yes	GDPR contract in place with supplier - have email confirmation		
c. All remote access by third party i.e. supplier maintenance / support is subject to formal approval and process management?	Yes	ULHT host the system and manage any remote access requests		
d. Does the commercial Third Party (CTP) hold ISO27001 or other recognised national accreditation?	Yes	Confirmation in Clinical Safety Case report		
e. The Commercial Third Party (CTP) holds a current IG assurance level on the IGTK or Data Security and Protection Toolkit (DSPT) or is working towards one - IG assurance should be enforced by the contract if necessary.	Yes	Supplier is GDPR compliant - have email confirmation		
11. Protection against malicious code				
a. Controls against malicious code are used or the system is protected by the host i.e. network and desktop controls.	Yes	Protected by host		
12. Business Continuity & Back Up Processes				
a. Full standard trust system back up process used	Yes	ULHT process		
b. System continuity configuration employed based on system criticality	Yes	Category 2		
c. A local BCP has been developed for the system /process	Yes	each organisation responsible for BCP		
d. If the system / service is managed by a third party is there a BCP and disaster recovery plan in place?	No	not applicable as day to day management is by ULHT		

13. Media Handling and Printing				
a. Does the system have the ability to print information? If so is printing required as part of the operational process?	Yes	No explicit print function available. Use of printed documents is dependent on each organisation's use of the portal. Printed documents have protective labelling on them.		
b. If printing is available but not required how is it to be managed - technical or organisational (policy) measures?	Yes	Organisation's policies to be followed - this is re-iterated in the e-learning package.		
c. Procedure are in place for the management of any removable media (including printed output) including handling, labelling and disposal	No	not applicable		
14. Exchange of Information				
a. All data transferred externally is encryption including electronic transfer or physical media	No	not applicable		
15. Operating System access control				
a. System admin password and accounts are limited to essential staff only	Yes	ULHT IT team manage this		
b. System configuration is limited to approved system administrators	Yes	ULHT IT team manage this		
16. Are medical devices being utilised?		**No**		
a. How is data stored, is it on the device or on an external device	No			
b. How can information be wiped prior to giving the device back to the company	No			
c. Is data encrypted on the device / external device	No			

Step 3 – Criteria for Privacy Law Compliance Checks

Senior executives of government agencies and company directors must ensure that the operations for which they are responsible comply with all relevant laws. The purpose of this section of the DPIA is to assist organisations in complying with privacy-related laws. The services of a legal professional with relevant expertise may be needed. If any of the following questions are answered "Yes", then a privacy law compliance check should be conducted:

Questions	Yes/No	Comments must be included to support your answer
1. Does the project involve any activities (including any data handling), that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act? In particular, the following laws and other forms of regulation should be considered, but the list may not be exhaustive.		
a. The Human Rights Act, in particular Schedule 1, Article 8 (right to respect for private and family life) and Article 14 (prohibition of discrimination)	Yes	GDPR compliance document has full details of relevant Acts.
b. The Regulation of Investigatory Powers Act 2000 (RIPA) and Lawful Business Practice Regulations 2000.	No	
c. The Privacy and Electronic Communications Regulations 2003 (PECR).	No	
d. The Data Retention (EC Directive) Regulations 2007.	No	
e. Statutes that impose regulatory conditions on the manner in which the organisation operates	No	
f. Sectoral legislation, eg Financial Services and Markets Act 2000.	No	
g. Statutory codes, eg the Information Commissioner's CCTV code of practice.	No	
Where projects are cross-jurisdictional the law of more than one country may be involved and other legal provisions may also need to be considered		
2. Does the project involve any activities (including any data handling) that are subject to common law constraints relevant to privacy? In particular, the following should be considered:		
a. Confidential data relating to a person, as that term would be understood under the common law duty of confidence	Yes	See previous sections of DPIA for further info. Also GDPR compliance document.
3. Does the project involve any activities (including any data handling) that are subject to less formal good practice requirements relevant to privacy? In particular, the following should be considered		
a. Industry standards, eg the ISO/IEC 27001:2013 Information Security Standard	Yes	Supplier is compliant as per their Clinical Safety Case report
b. Industry codes, eg the Guide to confidentiality in Health and Social Care.	Yes	
Privacy law compliance checking Organisations must continue with step four of the screening process, to determine whether Data Protection Act compliance checking also needs to be included in the project schedule. Note that compliance checking activities are usually conducted reasonably late in the overall project schedule, once detailed information about business processes and business rules is available		

Step 3 – GDPR Compliance Check

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with UK Data Protection legislation

Questions	Yes/No	Comments must be included to support your answer
Article 5(1)(a) - Principle 1 Personal data shall be processed fairly and lawfully and in a transparent manner in relation to the data subject		
a. Have you identified the purpose of the project?	Yes	
b. How will individuals be told about the use of their personal data?	Yes	see prev section
c. Do you need to amend your privacy notices?	No	
d. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.		
e. Has a lawful basis been established in accordance with Article 6 and 9	PCD2	
f. If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	Yes	Opt out consent model. If individual opts out data is not surfaced in the care portal
Article 5(1)(b) - Principle 2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes		
a. Does your project plan cover all of the purposes for processing personal data?	Yes	
b. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means		
c. Have potential new purposes been identified as the scope of the project expands?	Yes	
Article 5(1)(c) - Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.		
a. Is the information you are using of good enough quality for the purposes it is used for?	Yes	
b. Which personal data could you not use, without compromising the needs of the project?	No	
Article 5(1)(d) - Principle 4 Personal data shall be accurate and, where necessary, kept up to date.		
a. If you are procuring new software does it allow you to amend data when necessary?	No	
b. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Yes	Each org has DQ team. Care Portal's Patient Index functionality identifies DQ issues.
c. Will there be processes in place to ensure data is kept up to date?	No	Each org
Article 5(1)(e) - Principle 5 Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.		
a. What retention periods are suitable for the personal data you will be processing?	N/A	
b. Are you procuring software which will allow you to delete information in line with your retention periods?	N/A	
Article 5(1)(f) - Principle 6 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 ('integrity and confidentiality').		
a. Do any new systems provide protection against the security risks you have identified?	Yes	
b. What training and instructions are necessary to ensure that staff know how to operate a new system securely?	Yes	e-learning
Article 8 Conditions applicable to child's consent in relation to information society services		
a. Will the system make use of web services for children under the age of 16	No	
Article 15 Personal data shall be processed in accordance with the rights of data subjects under this legislation.		
a. The systems you are putting in place allow you to respond to subject access requests more easily?	No	
b. If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	Yes	see previous
c. Will the system allow you to amend data if the individual objects to the accuracy of that data? (Right to Rectification Article 16)	No	
d. Will the system allow you to remove data if the individual objects to the processing of that data? (Article 17)	No	
e. Will the system allow you to stop the processing of the data if the individual objects to the processing of that data? (Article 18)	Yes	
f. Will the system give the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. (Article 20)	No	
Article 46 A controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.		
a. Will the project require you to transfer data outside of the EU?	Within UK	
b. If you will be making transfers, how will you ensure that the data is adequately protected? In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.		