Data Protection Impact Assessment Screening Questions

The following screening questions will help our team decide whether a data protection impact assessment is required. * Further information is provided in the glossary of terms. Answering "**Yes**" to any of the screening questions below represents a potential Information Governance risk factor that may have to be further analysed to ensure those risks are identified, assessed and mitigated prior to the project being purchased and implemented. The decision whether to undertake a full Data Protection Impact Assessment will be supported by the Information Governance Lead and the Project Manager/Implementer.

No commitments to, or installation of systems, should take place before the assessment has been signed off.

The name of the project	
The name of the Information Asset Owner	
The name of the Information Asset Administrator	
The name of the project manager/Implementer	
Stakeholders/Third parties* if we are using a supplier please complete questions 1 -	

1. Overview of the Project (what the proposal aims to achieve)	
2. Will the project involve processing of information about individuals?	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5. Does the project involve using new technology being introduced?	

6. Does the project include any of the following data sets? (Mark all that apply)	**Personal data***	
	Pseudonymised data*	
	Anonymised data*	
	Education and training details*	
	Employment details*	
	Ethnicity and Race*	
	Financial details*	
	Goods or services*	
	Legal detail*	
	Political opinion	
	Religious or philosophical beliefs	
	Trade union membership	
	Genetics*	
	Biometrics*	
	Health data*	
	Sex life*	
	Criminal data*	
	Location data*	
	Family, lifestyle and social circumstances*	
	Vulnerable individuals*	
	Technology identifiers*	

7. Does the project include any of the following activities? (Mark all that apply)	**Evaluation or scoring - including profiling, predicting and transactional monitoring techniques. For example, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks; a new system that might be susceptible to fraud or abuse, and if so whether it ensures that the system has the capability for transactional level monitoring so you can audit the transactions if needed as part of an investigation.**	
	Automated decision making with legal or similar significant effect - processing that aims at taking decisions on individuals without human intervention. For example, the processing may lead to the exclusion or discrimination against individuals.	
	Systematic monitoring of individuals* (e.g. CCTV, body camera's, health data through wearable devices) processing used to observe, monitor or control individuals. For example, monitoring of the employees' work station, internet activity, etc.	
	Sensitive data or data of a highly personal nature - this includes special categories of personal data (for example information about individuals' health care, racial or ethnic origin etc.).	
	Data processed on a large scale – how many individuals concerned, either as a specific number or as a proportion of the relevant population; b. the volume of data and/or the range of different data items being processed; c. the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.	

	Matching or combining datasets - for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject	
	Data concerning vulnerable individuals - individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable individuals may include children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.).	
	Innovative use or applying new technological or organisational solutions - combining the use of finger print and face recognition for improved physical access control. Implementation of a new technology, system or business process or collection of new information	
	Preventing individuals from exercising a right or using a service or contract - When the processing in itself "prevents individuals from using a service or a contract". An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.	
	Offer online services directly to children	
	Storing or transferring data outside the EU (e.g. cloud computing, accessing data outside the EU, use of an American transcribe company)	
	Direct marketing (e.g. newsletters, postcards, telemarking, e-mail subscriptions)	

8. Is the project a replacement, new project or upgrade?	Replacement	New	Upgrade	Not applicable

9. Is there a requirement for interaction with other systems in the organisation? Please specify which systems ie CareFlow EPR, Nervecentre.	Yes (please list the systems)	No	Not applicable

10. Is it a medical device? If yes, is a Patient Safety Review required? DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital	Yes	No	Not applicable

The following questions (11 – 16) are to be answered if we are using a third party ie supplier

11. Is the supplier registered with the ICO? Please check the register	Yes	No

12. Has the supplier received ICO Enforcement? Please check the register	Yes	No

13. Has the supplier received ICO Decision Notice? Please check the register	Yes	No

14. Has the supplier received an ICO Audit? Please check the register	Yes	No

15. Has the supplier completed a Data Security and Protection Toolkit, please check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met

16. Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates		
	Yes	No
Cyber Essentials Plus/Cyber Assessment Framework (CAF)		
ISO 15489 Records Management		
ISO 27001 Information Security Standards		
ISO/IEC 27701:2019 Ext to 27001/27002		
ISO 9001 Quality Management Systems		
ISO 27017 Cloud Services		
ISO 27018 PII in public clouds		
Digital Technology Assessment Criteria for Health and Social Care (DTAC)		

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	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	Business continuity plan in place								
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					

Any risks scoring above 6 will need to be reviewed by the Senior Information Risk Owner (SIRO) & Data Protection Officer (DPO) or an approved deputy .

Assessment of the proposal against the GDPR 'High Risk' criteria requiring a DPIA

High Risk Processing (see glossary of terms below)		
Does the processing meet the criteria of 'high risk' processing?	Yes ☐	No ☐
Comments:		

Declaration

- **None of the screening questions apply to the project.**
- **Some of the screening questions apply to the project. I understand that the Data Protection Officer will need to be involved and a full data protection impact assessment will need to be completed.**

Name:

Job title:

Date:

Please note incomplete forms will be returned and not assessed

Glossary of Terms

Anonymised data	Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
Biometrics	Facial/voice recognition, fingerprints
Criminal data	convictions, outcomes, sentences including offences or alleged offences
Data matching	Combining, comparing or matching personal data obtained from multiple sources.
Education and training details	qualifications or certifications, training records
Employment details	career history, recruitment and termination details, attendance details, appraisals
Ethnicity and race	Race is often defined as being related to notions of intrinsic physical differences between groups of people. Race includes a person's skin colour, nationality and ethnic or national origins.
Family, lifestyle and social circumstances	marital status, housing, travel, leisure activities, membership of charities)
Financial details	banking, income, salary, assets, investments, payments
Genetics	DNA – an individual's gene sequence
Goods or services	contracts, licenses, agreements
Health data	treatment, diagnosis, medical information including a physical or mental health or condition
High risk (where a type of processing is likely to result in a high risk to the rights and freedoms of individuals. The potential for any significant physical, material or non-material harm to individuals)	nine criteria which may act as indicators of likely high risk processing: 1. Evaluation or scoring 2. Automated decision-making with legal or similar significant effect 3. Systematic monitoring 4. Sensitive data or data of a highly personal nature 5. Data processed on a large scale 6. Matching or combining datasets 7. Data concerning vulnerable data subjects 8. Innovative use or applying new technological or organisational solutions 9. Preventing data subjects from exercising a right or using a service or contract.
Large scale	the GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider: • the number of individuals concerned • the volume of data • the variety of data

	• the duration of the processing • the geographical extent of the processing. Examples of large-scale processing include: • a hospital (but not an individual doctor) processing patient data • a telephone or internet service provider processing user data
Legal detail	legal documents or agreements, court papers
Location data	GPS location, Wi-Fi tracking, vehicle tracking
Personal data	name, address, postcode, email address, date of birth, IP address, NHS number, National Insurance number, passport/driving licence numbers
Pseudonymised data	Pseudonymisation is defined within the GDPR as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information i.e NHS number, name, date of birth, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual”
Sex life	sexual health, sex life or sexual orientation
Systematic monitoring of individuals	• Audio/video surveillance of public areas • body camera’s • health data through wearable devices • automatic number plate recognition. • traffic management systems involving monitoring of vehicle/driver behaviour • Wi-Fi/Bluetooth/RFID tracking • Application of Artificial Intelligence
Technology identifiers	device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags
Vulnerable individuals	Children and persons who are 18 years of age or over, who may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself , or unable to protect himself against significant harm or serious exploitation