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

The name of the project	Step into Health
The name of the Information Asset Owner	Rob Symcox, Director of People
The name of the Information Asset Administrator	Rebecca Ford, Recruitment Manager, HR
The name of the project manager/Implementer	Rebecca Ford, Recruitment Manager, HR
Stakeholders/Third parties* if we are using a supplier please complete questions 1 -	NHS Confederation

1. Overview of the Project (what the proposal aims to achieve)	Step into Health is a programme created by NHS Confed, in conjunction with Walking with the Wounded and The Royal Foundation, which connects employers in the NHS to people from the Armed Forces community by offering an access route into employment and career development opportunities. An overview of the system is here Step into Health candidate system | NHS Employers This is something that many Trusts around the country have pledged to sign up to and is something that Sherwood Forest Hospitals are very keen to support themselves with many ex-military personnel offering a number of skills relevant to many roles around the Trust.

	At a time when we are finding it very difficult to recruit to many roles across all sectors this opens up more avenues to explore
2. Will the project involve processing of information about individuals?	Yes. The data from the Armed Forces community will be provided by the user when registering, this will include: • Date of Birth • Name • Armed Forces community description • Service number • Rank • Military branch • date of leaving or date available • current/preferred location • job type • role area of interest • type of work you are looking for • source of referral.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	The Trust will be able to record engagements with individuals including: • Details of phone calls • Work placements • Event meetings The Trust will be able to refer candidates to other employers via email, although no data will leave the system, they will receive a notification prompting them to log into the tool. The Trust and NHS Confederation have a data sharing agreement. The Trust will have control of who has access to the data and this will be reviewed on a 6 monthly basis.

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?	Yes. Users invited to sign up to Step into Health must complete the registration form before their details are saved. If a user ignores the invitation email and does not register within defined period the system will delete their details. SITH-Privacy-Notice.docx (live.com). As part of the registration process we will ask them to agree to their data being shared and how it will be used. https://vimeo.com/nhsemployers?embedded=true&source=video_title&owner=28612472
5. Does the project involve using new technology being introduced?	No

6. Does the project include any of the following data sets? (Mark all that apply)	**Personal data***	x
	Pseudonymised data*	
	Anonymised data*	
	Education and training details*	x
	Employment details*	x
	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
		x		

9. Is there a requirement for interaction with other systems in the organisation? Please specify.	Yes (please list the systems)	No	Not applicable
		Currently NHS Confederation are not exploring a link to TRAC/NHS Jobs as the majority of the interventions recorded by the tool will cover the pre-employment side of a candidates journey. Once they apply for roles and are offer TRAC/NHS Jobs adequately cover this.	

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
			x

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
	Z9002192	

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

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

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

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
	No		

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		X
ISO 15489 Records Management		X
ISO 27001 Information Security Standards		X
ISO 9001 Quality Management Systems		X

DPIA Risk Assessment

17. Are there any risks to the Confidentiality of personal data? Confidentiality is defined as unauthorised disclosure of, or access to, personal data.

Data is entered by the data subject and the Trust.

Risk - Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed.

Mitigation - Username and password controls in place and access is managed by the Trust. The system has a chronological audit trail of user logins which are date/time stamped.

18. Are there any risks to the Integrity of personal data? Integrity is defined as unauthorised or accidental alteration of personal data.

No, the data is entered by the data subject and the Trust. We would expect that data subjects include accurate information and the individual's data will be kept up to date by them.

19. Are there any risks to the Availability of personal data? Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.

The data will all be held on a secure HSCN server. Regular backups of the database will be completed.

Risk - Loss of system data due to system failure and/or backup failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be reputational damage to the Trust.

Mitigation - Full system back-up processes in place with NHIS and NHS Confederation.

20. Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?

No financial information will be recorded on the tool. The system has a chronological audit trail of user logins which are date/time stamped.

21. If the answer is "Yes" to 17, 18, 19 or 20, how are these to be Reduced or Mitigated?

As described above in 17 – 20.

22. Once the mitigations in 17 to 20 are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Consequence. Further guidance available here.

Likelihood *(please tick)*				**Consequence** *(please tick)*				
1		Very Unlikely	**x**	**1**	x	Very Low	**=**	2
2	x	Unlikely		**2**		Low		
3		Possible		**3**		Moderate		
4		Somewhat Likely		**4**		High		
5		Very Likely		**5**		Very High		

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

- **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 may need to be completed.**

Name: Robert Symcox

Job title: Director of People

Date: 17th October 2022

Name: Jacquie Widdowson

Job title: Information Governance Manager and Data Protection Officer

Date: 18th October 2022

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, 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