IG-DPIA NO:	DPIA-152	**IGT TSK NO:**	
ISA NO:		**IGT TSK NO:**	

INDEX			
Tab 1	Introduction		
Tab 2	Information Governance - General (Q1 to Q34)		
Tab 3	Information Governance - Security (Q35 to Q49)		
Tab 4	Identified Risks		
Tab 5	Recommendations & Signatures		
Tab 6	Reference Tab		

IG-DPIA NO:	DPIA-152 IGT-128296		Ref. SRV-127928
ISA NO:			

DATA PROTECTION IMPACT ASSESSMENT

Under GDPR, it is now a legal requirement that a Data Protection Impact Assessment (DPIA) is completed at the start of ALL projects (major and minor) involving the use of personal data or significant changes are being made to an existing process or project. ALL final outcomes should be integrated back into the project and process.

This tool must be completed if there is a change to an existing service/technology or a new process/technology or service that could involve a new use or significant changes to how personal data is handled or processed.

Title of Project / Process:	Use of TreeSize software		
New DPIA	Yes		
Customers/Stakeholders *(Full name(s), department(s) and contact details of all Customers/Stakeholders)*	[redacted]		
Project Lead: *(Full name, job title and contact details)*			
Proposed start date for the project or processing to commence	ASAP (already in use by Infrastructure)		
If project or processing of data has already commenced, please give your reasons for not previously completed a DPIA (formerly called Privacy Impact Assessment).			
DPIA Conducted by:	[redacted]	Information Security Analyst	

SUMMARY OF THE PROJECT/PROCESS **Please give a brief summary of:**	
What is the purpose of the project?	To use the software to determine where space can be maximised on a users machine
What the project aims to achieve?	
What are the benefits provided by the project?	Easier to rectify times in a given timeframe
What is the intended effect on individuals?	Jobs get completed quicker with users happier
What is the nature of your relationship with the individuals?	Former colleagues
How much control will the individuals have over the project/process?	Complete
Will this project/process include dealing with children or other vulnerable groups?	

What type of processing does it involve?	

INFORMATION GOVERNANCE:						STATUS			
						High	Significant	Moderate	Low
1	What is the nature of the data and does this include special category or criminal offence(including alleged offences) data? *(Please select all those appropriate)*	Personal ☐	Special Category ☐	Criminal Offence ☐	Corporate Sensitive ☐				
2	What is the source of the data? *(Please select all those appropriate)*	Patient ☐	Staff ☐	Other ☐					
3	Describe how the system/project/process will collect personal data, special category data or corporately sensitive data that has not been collected before?								
4	Is the information being used for a different purpose to currently being used?		If yes, please give details						
5	Is the information collected likely to raise additional privacy concerns or expectations This is above and beyond the routine processing of special category date		If yes, please give details						
6	Will the project require you to contact individuals in ways which they may find intrusive?		If yes, please give details						
7	Does the system/project/process results in decisions being made, or action being taken, against individuals in ways which can have a significant impact on them *Where fully automated decision making is involved this is to be treated as a SIGNIFICANT risk*	Decisions made ☐	Actions taken ☐	Significant impact ☐					
8	Describe the checks that have been carried out regarding adequacy, relevance and necessity for the collection of personal and sensitive data for this system/project/process?								

9	Any other information we need to be aware of?					
	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO approval					

ACCESSING DATA

10	Is access required to internal or external systems? *Please select all which apply*							
11	Describe the authorisation process if accessing an external system							
12	What level of access will be authorised to the system/process/project?	Read Only: ☐	Modify: ☐	Full Control: ☐	Other: ☐			
13	Describe how the access to data will be managed Please explain in full detail							
14	Who will create the accounts? *Please give full details of name/job title/area/department/organisation if not NSFT*							
15	Who will be accessing the system/project/ process? *Please give details of name, job title, dept /service, location and number of people requiring access*							
16	Is there any other information we need to be aware of?							

RETENTION AND DISPOSAL OF DATA

17	What geographical area does the data cover?						
18	Describe how long the data will be kept and how it will be stored						
19	Describe how the data will be disposed of						
20	Describe how the data will be transferred to a new service provider (if applicable)						
21	Will data be sent off site?		If yes, please give details				
22	Describe the process of data portability for the system/project/process *Include information on plans in place regarding archiving/transferring/disposing of information should the system/project/process stop*						
23	Is there any other information we need to be aware of?						

COMPLYING WITH THE LAW

24	Does this processing fall within our lawful reasons? *Please select all which apply*	Article 6 (1)	Article 9 (2)				
		b ☐	b ☐	h ☐			
		c ☐	c ☐	i ☐			

		d ☐	f ☐	j ☐				
		e ☐	g ☐					
25	Will the data be shared with anyone who have not previously had reason to access it?							
26	Who are the Data Controllers and Data Processors							
27	Are the organisations registered with the ICO?		If yes, please give registration number: In no, please give reasons:					
28	Do the organisations complete the DSP Toolkit?		If yes, please give registration number: In no, please give reasons:					
29	Are the organisations ISO 27001 certified?		If yes, please give registration number:					
30	Describe the data security and protection requirements that have been defined between NSFT and the other controllers and processors							
31	Do the contracts contain all the necessary IG clauses regarding Data Protection and Freedom of Information		If yes - copy required If no, please give reasons:					
32	Will the data be sent outside the European Economic Area (EEA)?		If yes, list countries involved					
33	Are procedures in place to prevent processing for direct		If yes, please give details:					

33	marketing?		If no, how is it prevented:				
34	Is there any other information we need to be aware of?						

TECHNOLOGY:				STATUS				
				High	Significant	Moderate	Low	Insignificant
35	Describe the technical configuration of the system/project/process *(include support & administration, tracking technologies, database structures such as SQL, security by design measures such as redundancy, single points of failure, back up)*	The Software (professional) licence is procured then the latest version is downloaded for https://www.jam-software.com and then the techs use the software to scan a target device, no data is taken from the machine the techs can just see that 8GB for example is being used by outlook. The information can be gained another way but that take several hours where the software takes minutes. This us currently used by Infrastructure for hte past 10 years						
36	Describe the security measures that have been put in place (or will be in place) to secure access to and limit the use of the data *(such as username and password, smartcard, locked filing cabinets/room, restricted access to network files)*	The software is installed on the techs machine which he/she access by their domain username and password, the licence is specific to a single user per single licence. No data is transmitted off the device.						
37	If new technology, does it employ approved encryption standards for data at rest or in transit? *E.g. 256bit AES encryption*	Yes	256 AES encryption used If no, give details of other encryption standards used					
38	If new technology does it share a commonly recognised secure platform? *E.g. Office 365, Microsoft SharePoint, encrypted email*	Yes	It uses the msinfo logs to conduct the searches needed					
39	If new technology, might it be perceived as intrusive to privacy? *(facial recognition or biometrics)*	No	If yes, give details:					
40	Are there any technical concerns that warrant further follow up?	No	If yes, explain further					
41	Does the system/project/process have an audit trail?	Yes	Logpoint logs all changes made to registry and log ons/off If no, explain how the systems are audited:					
42	Is this software/technology or similar already is use within the organisation?		If yes, give details of the technology involved and is the soft hosted on local or external servers					

43	Who will be the Information Asset Owner (IAO) and Asset Administration(s)? *(name, job title and contact details)*							
44	Is there a Business Continuity Plan (BCP) in place for the system/project/process	No	If yes, list BCP Ref. Number: Not needed					
45	Is there a Disaster Recovery Plan (DRP) in place for the system/project/process	No	If yes, list DR Ref. Number: No not needed					
46	Is the data being retrieved by a personal identifier *e.g. RMY Number, NHS Number, NI number)*	No	If yes, give details: N/A					
47	Will formal staff training be required before accessing the data?	No	If yes, give details of what is required and numbers:					
48	Does the system/project/process involve pulling together information about people from difference places, linking it, cross-referencing?	No	If yes, give details:					
49	Is there any other information we need to be aware of?	No, apart from software has been used for the last ten years by infrastructure, with the principle analyst being new to post he has raised the need for a DPIA before he can purchase a licence for the remote support team						
	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO approval							

IDENTIFIED RISKS

Information Governance section	
Have all the questions been answered satisfactory	
Is further investigation required?	
Completed by (Name):	

Information Security Section	
Have all the questions been answered satisfactory	
Is further investigation required?	
Completed by (Name):	

The following risks have been identified and are to be managed in accordance with the Trust's Risk Management Strategy.

IMPORTANT: The Data Protection Officer and/or the Senior Information Risk Officer are required to review/approve the DPIA, subject to the identified risks being mitigated.

PROCESSING MUST NOT COMMENCE UNTIL THESE RISKS ARER MITIGATED AT THE RIGHT LEVEL

Risk No	1			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	2			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	3			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	4			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

*** Consequence x impact = rating**
**** Consequence x impact = rating**

Risk No	5			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

*** Consequence x impact = rating**
**** Consequence x impact = rating**

RECOMMENDATIONS AND RISKS		
It is recommended that: *Select as appropriate*	An Information Sharing Agreement is created	☐
	The DPO/SIRO accepts these recommendations and risks and permits the processing to proceed	☐
	The DPO/SIRO DOES NOT permit the processing as described. This would be subject to further mitigation of the HIGH RISKS	☐

APPROVAL-DATA PROTECTION OFFICER	
As Data Protection Officer, I confirm that the highest level of risk identified in this DPIA is:	Insignificant
Processing may commence. The risks are proportionate and they can be managed accordingly.	☐
Processing MUST NOT commence. Further mitigating actions are required.	☐
Additional Comments	
Name	**Richard Green**
Signed/email date	**10/10/2019**

APPROVAL-SENIOR INFORMATION RISK OWNER	
As Senior Information Risk Owner, I confirm that the highest level of risk identified in this DPIA is:	
Processing may commence. The risks are proportionate and they can be managed accordingly.	☐
Processing MUST NOT commence. Further mitigating actions are required.	☐
Additional Comments	
Name	
Signed/email date	

DATA & NSFT'S LAWFUL BASIS TO PROCESS

GDPR Article (Personal Data)

What is Personal Data?	Any information relating to an identified or identifiable natural person ('data subject')
What is an identifiable natural person?	One who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
What information can be an identifier?	Name, Identification number, Location data, Online identifiers (internet protocol (P) addresses, cookie identifiers, radio frequency identification (RFID) tags, MAC addresses, Advertising IDs, Pixel tags, Account handles, Device fingerprints

Article 6 (1) (b)	Processing is necessary for a contact you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6 (1) (c)	Processing is necessary for us to comply with the law (not including contractual obligations)
Article 6 (1) (d)	Processing is necessary to protect someone's life
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

GDPR Article (Special Categories of Data)

What is Special Category Data?	Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade Union membership, Genetic Data/Biometric data, Health date, Sexual orientation

Article 9 (2) (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 and social security and social protection law
Article 9 (2) (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person
Article 9 (2) (f)	Processing is necessary for the establishment, exercise or defence of legal claims or courts acting in judicial capacity
Article 9 (2) (g)	Processing is necessary for reasons of substantial public interest
Article 9 (2) (h)	Processing is necessary for the purposes of preventive and 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
Article 9 (2) (i)	Processing is necessary for reasons of public interest in the area of public health or ensuring health standards of quality and safety of health care and of medicinal products or medical devices
Article9 (2) (j)	Processing is necessary for scientific or historical research purposes or statistical purposes

RISK ANALYSIS TOOL

PART 1 - RISK CONSEQUENCE GRADING

GRADES		OUTCOME/SEVERITY						
Grade	**Category**	**Safety**	**Quality**	**Statutory Duty**	**Information Governance**	**Service Continuity**	**Finance**	**Reputation**
5	**CATASTROPHIC**	Fatality/Fatalities	Totally unacceptable treatment or service	Multiple breaches in statutory study	Inevitable Data Privacy Breach	Permanent loss of service or facility	>£10M	National media coverage for 3 or more days
		Multiple Permanent injuries or irreversible health effects	Gross failure to meet national professional standards	Sustained failure to meet national professional standards	Processing must not commence or cease immediately	Catastrophic impact on the environment		Total loss of public confidence
		Impacts a large number of people	Ombudsman injury	Prosecution	Mitigating action or solution to unacceptable risk will be required			Questions in the House
			Inquest		Data Protection Officer must be involved			
					Individuals Affected: 1,000+			
					Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: Will identify individual (s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			

4	**MAJOR**	Permanent or long-term incapacity/ disability	Unacceptable treatment of service	Multiple breaches in statutory duty	High chance of Data Privacy being compromised	Loss of service or facility > 1 week	£1m - £10M	National media coverage for less than 3 days
		Length of hospital stay increased by > 15 days	Non-compliance with national standards	Intermittent failure to meet professional standards	Mitigating action or solution to unacceptable risk will be required	Moderate impact on the environment		Service well below public expectation
		> 14 days off work	Independent review	Improvement notices	Individuals Affected: 100-1 000			
			Critical report	Enforcement action	Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: High Possibility of identifying individual(s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
					Data Protection Officer must be involved			
3	**MODERATE**	Injury requiring professional intervention	Significantly reduced effectiveness of treatment of service	Failure to meet internal professional standards and/or national performance standards	Moderate chance of Data Privacy being compromised	Loss of service or facility > 1 day	£100K - £1M	Local media coverage
		RIDDOR reportable	Formal complaint (stage 2)	Civil action for negligence	Mitigating actions to be implemented to reduce risk to accepted level.	Moderate impact on the environment		Long-term reduction in public confidence
		Length of hospital stay increased by 4-15 days	Potential to go to independent review		Individuals Affected: 11-100			
		7-14 days off work			Reporting Requirements: Internal reporting and MAY need reporting to ICO			
					Sensitivity Factor: possibility of identifying individual (s)			
					Financial Penalty Risk: May lead to serious * fines from ICO			
					Data Protection Officer to be made aware			
2	**MINOR**	Minor injury dealt with one site (first aid)	Suboptimal overall treatment or service	Failure to meet internal professional standards	Minor chance of Data Privacy being compromised	Loss of service or facility > 8 hours	£5K to £100K	Local media coverage
		Length of hospital stay increased by 1 - 3 days	Formal complaint (stage 1)		Risk has been accepted or require minimal mitigating actions to rectify	Minor impact on the environment		Short-term reduction in public confidence
		Under 7 days off work	Local resolution		Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			
1	**INSIGNIFICANT**	Minimal injury requiring no treatment	Suboptimal peripheral treatment or service	Minor breach of internal professional standards	No/Low impact Risks to Data Privacy	Loss of service or facility <1 hour	<£5K	Rumours
			Informal complaint/inquiry		Identified Risks requiring no/minimal intervention	Minimal or no impact on the environment		Potential for public concern
					Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			

* The ICO will determine the fine based on a two-tiered sanction regime – lesser fines equate a max of €10 million or 2% of organization's global turnover.
** The ICO will determine the fine based on a two-tiered sanction regime – serious fines equate a max of €20 million or 4% of organization's global turnover.

PART 2 - RISK RATING MATRIX

To rate a risk

1 Risk Consequence Grading (Part 1)
2 Grade the likelihood (Part 2)
3 Multiply this consequence (1-5) by the likelihood (1-5) to get the risk rating

		LIKELIHOOD				
		5	4	3	2	1
		Almost Certain	Likely	Possible	Unlikely	Rare
		Will undoubtedly happen, possible frequently	Will probably happen, but not persistently	Might happen occasionally	Not expected to happen, but could do so	May occur only in exceptional circumstances
CONSEQUENCE	5 Catastrophic	25	20	15	10	5
	4 Major	20	16	12	8	4
	3 Moderate	15	12	9	6	3
	2 Minor	10	8	6	4	2
	1 Insignificant	5	4	3	2	1

PART 3 - RISK MANAGEMENT - ACTION AND TIMESCALES

Risk Level	Action and Timescales
HIGH 15 - 25	Immediate action must be taken to manage and mitigate the risk. Control measures should be put into place to reduce the consequence of the risk or the likelihood of it occurring. A number of control measures may be required and significant resources may have to be allocated to reduce the risk.
SIGNIFICANT 8 - 12	Efforts should be made to reduce the risk but the cost of prevention should be measured and weighed against the consequence of the risk. Establish more precisely the likelihood of harm as a basis for determining the need for improved controls.
MODERATE 4 - 6	The likelihood of harm should be established before implementing further controls. Existing controls should be monitored and consideration should be given to a more cost-effective solution that imposes no additional cost.
LOW 1 - 3	Acceptable risk, no further action or additional controls are required. A risk at this level should be monitored, and reassessed at appropriate internals to ensure that it has not worsened.

Risk Analysis Tool taken from Q18 - Risk Management Strategy - Version 05 - dated 23rd March 2018

IG-DPIA NO:	DPIA-108	**IGT TSK NO:**	IGT-114884
ISA NO:	**NO ISA IS REQUIRED TO BE CREATED, THIS DPIA COVERS PROCESSES AND PROCEDURES ONLY.**		

INDEX			
Tab 1	Introduction		
Tab 2	Information Governance - General (Q1 to Q34)		
Tab 3	Information Governance - Security (Q35 to Q49)		
Tab 4	Identified Risks		
Tab 5	Recommendations & Signatures		
Tab 6	Reference Tab		

IG-DPIA NO:	DPIA-108	**IGT TSK NO:**	IGT-114884
ISA NO:	**NO ISA IS REQUIRED TO BE CREATED, THIS DPIA COVERS PROCESSES AND PROCEDURES ONLY.**		

DATA PROTECTION IMPACT ASSESSMENT

Under GDPR, it is now a legal requirement that a Data Protection Impact Assessment (DPIA) is completed at the start of ALL projects (major and minor) involving the use of personal data or significant changes are being made to an existing process or project. ALL final outcomes should be integrated back into the project and process.

This tool must be completed if there is a change to an existing service/technology or a new process/technology or service that could involve a new use or significant changes to how personal data is handled or processed.

Title of Project / Process:	Health Research Authority (HRA)-Approved Research Studies		
New DPIA	Yes	If no, insert previous DPIA number:	
Customers/Stakeholders *(Full name(s), department(s) and contact details of all Customers/Stakeholders)*	Name: Research and Development,	Hellesdon Hospital, Drayton High Road, Norwich, NR6 5BE	Contact details Phone: 01603 421340 Email: Research@nsft.nhs.uk
Project Lead: *(Full name, job title and contact details)*	Name: [redacted]	Research and Development, Hellesdon Hospital, NR6 5BE	Contact details: Phone|: 01603 421340 Email - Research@nsft.nhs.uk
Proposed start date for the project or processing to commence	Ongoing Activity		
If project or processing of data has already commenced, please give your reasons for not previously completed a DPIA (formerly called Privacy Impact Assessment).	DPIA was completed for specific research projects, but on review, the processes and procedures for each research studies are the same, so it has been decided to have an overarching DPIA for all research studies, apart from those which fall outside the scope of these arrangements.		
	Name: [redacted]	Job Title: [redacted]	Contact details: [redacted]

DPIA Conducted by:	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

SUMMARY OF THE PROJECT/PROCESS **Please give a brief summary of:** **This DPIA has been produced to cover the processes and procedures which each research study follows when research studies are being considered. Each study will involve different partners and participants but the processes and procedures will always follow the same pattern after approval has been received from the Health Research Authority (HRA). The current list of research projects undertaken since GDPR went live is attached on Tab 5. Recommendations and Signatures under Additional Comments.**	
What is the purpose of the project?	All research studies taking place in NSFT are required to obtain national Health Research Authority (HRA) approval prior to their start. The HRA assessment includes a central review of how each individual research study complies to GDPR and Data Protection through researchers completing a standard research application form (IRAS). This project is to provide assurance as to the general data arrangements made for all research studies which take place in NSFT.
What the project aims to achieve?	By their nature, research studies involve the collection of data from service users, carers and staff (collectively called Participants) for the purposes of evaluation of healthcare services, conditions, treatments and care. This data is primarily obtained directly from participants with explicit research consent via face-to-face or online methods. Occasionally, routine clinically collected data may also be obtained as part of a research study. Given that HRA-approved research tends to be a national-level collaboration across health and university partners, HRA approval may be given for the sharing of personal information of participants between NSFT and the Main Research Team (sponsor). This sharing of information is required to be only on the condition that participants provide permission for this personal data to be shared.

What are the benefits provided by the project?	Clinical research is associated with improved health outcomes, improved care and treatments. It is part of the NHS Constitution and evidence of involvement in research is part of the CQC well-led indicators. As part of the national research model, data collected by NSFT is collated with data shared with other participating NHS organisations at a central site (usually the study sponsor/data controller) as part of research protocols. The transfer of this information can be via secure post, email or online data portals.
What is the intended effect on individuals?	There are two broad types of research studies that NSFT is involved in: Observational (data collection only) or Interventional (change in care). Interventional studies test new forms of care (drugs, therapy etc) and may or may not have a direct benefit on the clinical outcomes and wellbeing of participants. Observational studies do not tend to have a direct benefit to participants, but the information collected is generally used to inform future care.
What is the nature of your relationship with the individuals?	NSFT is providing a research service to service users, carers, staff and other members of the public, which is separate to their routine clinical care (aside from risk assessment procedures where we liaise with clinical care providers).
How much control will the individuals have over the project/process?	Participants in research studies provide voluntary consent to take part - not taking part does not affect their clinical treatment for observational studies. They are free to withdraw at any time. The individuals are fully informed of what data is collected and where it will be shared and the reason for sharing via participant information sheets.
Will this project/process include dealing with children or other vulnerable groups?	Yes - Some research studies involve children and people who may lack capacity to consent for themselves. In these cases, additional arrangements are in place to obtain a valid consent/consultee permission in accordance with Section 30-34 of the mental capacity act.
What type of processing does it involve?	Step 1: Arrangements for data collection and sharing are completed by the Data Controller (via Lead Researcher) on the IRAS Application Form, in preparation for submission to the national Health Research Authority. Step 2: Once study is given HRA Approval, the documentation set, including IRAS form, is made available to NSFT R&D. Step 3: NSFT R&D gives a confirmation of capacity and capability for the study, and reviews local data arrangements and access to systems. Step 4 - Data Collection: If information is collected face-to-face: Research Practitioners in NSFT obtain voluntarily given information, including contact details (name, DOB, address, diagnosis etc) which is recorded in research case report forms. This personal information is NOT usually shared with the Sponsor/Data Controller unless HRA has provided approval for information to be shared. If information is collected via online only: Personal data to be collected is explicitly shared before any information has been entered by the participant. The participant can choose to share their personal information or not.

INFORMATION GOVERNANCE:						STATUS			
						High	Significant	Moderate	Low
1	What is the nature of the data and does this include special category or criminal offence(including alleged offences) data? *(Please select all those appropriate)*	Personal ☑	Special Category ☑	Criminal Offence ☐	Corporate Sensitive ☐				
		Personal contact information and blood/saliva samples may be collected by NSFT staff for research purposes depending on the requirements of the research study. Information is also requested from clinicians as researchers undertake assessments in people's homes and a level of risk assessment is required to enable lone working and community practice (NSFT service users only). Special Category - ethnicity, diagnosis may be asked as a result of research demographic requirements for certain studies. Research department also collects ethnicity/faith/age/gender in an anonymised format only (unlinked to research studies) for the purposes of equality/diversity service access needs.							
2	What is the source of the data? *(Please select all those appropriate)*	Patient ☑	Staff ☑	Other ☑					
		Personal information is collected from research participants and their study partners (carers) in the form of Name, Address, Contact Details and Date of Birth. This may be verified with clinical notes where participants are NSFT service users.							
3	Describe how the system/project/process will collect personal data, special category data or corporately sensitive data that has not been collected before?	The clinical care team members first approach potential participants to tell them about the study and provide an approved participant information sheet (unless the potential participant has already consented to be contacted directly about research studies). If the potential participants are interested, contact details are passed to the research team (NSFT research staff) who will then contact the participants to arrange a research assessment. This research assessment will obtain research consent to take part in the study and collect both identifiable data and potentially DNA or blood samples as per protocol. Data is provided by participants voluntarily, as evidenced by signed consent/assent forms. Special category data for participants may be collected for some studies in the form of ethnic origin, health and genetic data. This information is collected for research purposes in the public interest and will be stored in a linked-anonymised format. No special category data is collected for study partners. Additionally, the NSFT Research department collects anonymised demographic information only (age, ethnicity, faith, first 4 digits of postcode) for the purposes of assessing accessibility to research studies in underrepresented communities. This is held internal to NSFT only, and is not linked to personal data. Every person consented into research has their personal details held on a central recruitment log only accessible by NSFT-employed staff members. This is to be able to share study activities, have a validated point of contact and arrange appointments for all studies across department members. It is also recorded whether participants wish to be offered further research, if they wish to receive a newsletter/updates.							

4	Is the information being used for a different purpose to currently being used?	Yes	If yes, please give details: Personal information is collected for the purposes of arranging research appointment and communicating before and after the appointment. We will use this information to contact research participants in the future regarding new or follow-up research opportunities and newsletters with study updates only if they have agreed for the research team to do so (as specified in the consent form), for up to 15 years following the completion of the study. If they do not agree to follow-up research or to receipt of newsletter their personal information will be destroyed at the end of the study. Personal information is required throughout the duration of the study in order to address and data queries that may arise in this time. Special category data for participants will be collected in the form of ethnic origin, health and genetic data. This information is collected for research purposes in the public interest and will be stored in a linked-anonymised format. No special category data is collected for study partners.					
5	Is the information collected likely to raise additional privacy concerns or expectations This is above and beyond the routine processing of special category date	No	No. All personal data collected is used internally only. Personal information shared outside of the Trust is only for specific research studies and where both national and individual permission has been obtained for the sharing of this information. This purpose is usually for future contact only.					
6	Will the project require you to contact individuals in ways which they may find intrusive?	Possible	If yes, please give details: Potentially yes, depending on the circumstances of the study. Most work is in people's own homes, and we need to ask in-depth questions and (depending on the study) take blood/saliva samples. Participants have the choice as to how we communicate with them, via telephone/text/email etc. This is recorded on the research department's screening log.					
7	Does the system/project/process results in decisions being made, or action being taken, against individuals in ways which can have a significant impact on them *Where fully automated decision making is involved this is to be treated as a SIGNIFICANT risk*	Decisions made ☑	Actions taken ☐	Significant impact ☐				
		The patient and carer will be making their own decisions with supporting documentation and open discussion about whether to take part in a research study or not. A consultee can consent on behalf of the patient which will be documented on a consultee declaration form. At any point after this, they can make decisions about whether to continue in the study or not. All researchers have received training about speaking to participants in a non-cohersive way which does not restrict their rights or ability to make decisions for themselves. All researchers have received training about maintaining confidentiality of data.					

8	Describe the checks that have been carried out regarding adequacy, relevance and necessity for the collection of personal and sensitive data for this system/project/process?	The processes and procedures have been reviewed by the following bodies: NHS Ethical Committee (national), Health Research Authority (national). This includes an assessment of risk, data protection and intrusion, burden, risk vs benefit etc as well as compliance to GDPR. The studies has been granted approval from NHS Ethical Committee and Health Research Authorities.				
9	Any other information we need to be aware of?	The study may be subject to routine research audits and submission of progress reports, where data collection procedures and processes will be under scrutiny, in terms of adherence to agreed protocols. Paper copies of research documentation are held in locked cabinets within Norfolk and Suffolk NHS Foundation Trust research offices. Personal identifiable information collected as part of the study (i.e. consent forms, contact details) are stored in separate locked cabinets from any research data. All research data and blood samples are stored using anonymous ID numbers. Where personal data is required by protocol to be sent outside the Trust, and the person has provided permission for this. This can happen 1 of multiple ways: Secure mail, Secure email or via authorised online data portals/data systems which are managed through Clinical Trial Units (PROSPECT, REDCAP, REDPILL). Information is held in accordance with GDPR and NSFT's confidentiality policy. Any staff working with participants and/or personal identifying information are required to sign a confidentiality agreement as a term of their employment.				

ACCESSING DATA

10	Is access required to internal or external systems? *Please select all which apply*	Both					
11	Describe the authorisation process if accessing an external system	External system authorisation is granted by the Sponsor organisation and/or the Clinical Trials Unit which provides access to NSFT practitioners who are registered on study delegation logs. Access is shared with non-NSFT staff who have a letter of access or honorary research contract to enable access to any personal information on the site. Internal system authorisation is limited to people working within the NSFT Research Office only, and who have been granted access to ICT systems (CRN Research Studies Drive) via ICT.					
12	What level of access will be authorised to the system/process/project?	Read Only: ☐	Modify: ☑	Full Control: ☐	Other: ☐		
		Data is entered onto electronic systems by NSFT Research Practitioners using information provided from research assessments.					
13	Describe how the access to data will be managed Please explain in full detail	Access to non-NSFT electronic systems is granted by the Study Data Controller, who informs the Clinical Trials Unit (Contracted by the Data Controller to provide research database services) to setup NSFT Practitioners with individual log-ins and passwords for the purposes of research data entry.					

14	Who will create the accounts? *Please give full details of name/job title/area/department/organisation if not NSFT*	Access to non-NSFT electronic systems is granted by the Study Data Controller, who informs the Clinical Trials Unit (Contracted by the Data Controller to provide research database services) to setup NSFT Practitioners with individual log-ins and passwords for the purposes of research data entry.				
15	Who will be accessing the system/project/ process? *Please give details of name, job title, dept /service, location and number of people requiring access*	Within NSFT: Only research practitioners who have been listed on the study delegation of duties log to be working on the study and collecting data for the purposes of the study.				
16	Is there any other information we need to be aware of?	There are two main electronic database systems currently in use: PROSPECT (used by University of Sheffield) https://ctru-prospect.shef.ac.uk and REDCAP (Used by University of East Anglia) https://www.project-redcap.org/. REDPILL guidance is attached to this form. Clinical Trials Unit are contracted to provide research database systems, so that Data Controllers can access approved participant data as agreed by the Health Research Authority. Each CTU is required to have secure policies and systems in place to facilitate the use of these programmes nationally.				

RETENTION AND DISPOSAL OF DATA

17	What geographical area does the data cover?	Norfolk and Suffolk				
18	Describe how long the data will be kept and how it will be stored	Research data is usually stored for 10 years in NSFT Health Record Facilities (as per NSFT Research Archiving policy) in line with study protocols. Paper copies of study data are held within NSFT Health Records (personal data is marked separately and archived in different boxes). Electronic Data is archived via NSFT ICT drives, accessible only by Head of Research and the Senior Research Facilitator.				
19	Describe how the data will be disposed of	It will be subject to secure disposal by NSFT health records as per destruction policies.				
20	Describe how the data will be transferred to a new service provider (if applicable)	N/A				
21	Will data be sent off site?	Possible	If yes, please give details: If required, data is sent off site electronically via electronic databases (PROSPECT, REDCAP) and exceptionally via secure email. The latter may include referrals made for research studies to study-specific university researchers by clinical teams or research team members, if this process has been approved by the HRA.			
22	Describe the process of data portability for the system/project/process *Include information on plans in place regarding archiving/transferring/disposing of information should the system/project/process stop*	Personal data is stored in accordance to sponsor institution/data controller. Personal data may be stored at NSFT (through Health Records in accordance with R&D Archiving Policy) or will be collected by courier to be archived off-site by the Sponsor. The latter process has been granted permission by the HRA.				
23	Is there any other information we need to be aware of?					

COMPLYING WITH THE LAW

24	Does this processing fall within our lawful reasons? *Please select all which apply*	Article 6 (1)	Article 9 (2)					
		b ☐	b ☐	h ☐				
		c ☐	c ☐	i ☐				
		d ☐	f ☐	j ☑				
		e ☑	g ☐					
25	Will the data be shared with anyone who have not previously had reason to access it?	Yes						
		For research purposes						
26	Who are the Data Controllers and Data Processors	Whichever Organisation is sponsoring the study (NSFT, other NHS Trust, university).						
		Data Processor: All named research study team members as stated on the delegation log of each individual study.						
27	Are the organisations registered with the ICO?	Unknown	If yes, please give registration number: The Registration number for each organisation carrying out the research will be given at the time the research project is considered					
			In no, please give reasons:					
28	Do the organisations complete the DSP Toolkit?	Unknown	If yes, please give registration number: The Registration number for each organisation carrying out the research will be given at the time the research project is considered					
			In no, please give reasons:					
29	Are the organisations ISO 27001 certified?	Unknown	If yes, please give registration number: If the organisation carrying out the research this will be given at the time the research project is considered					
30	Describe the data security and protection requirements that have been defined between NSFT and the other controllers and processors	Stated in each IRAS form prepared by Research Sponsor organisation.						

31	Do the contracts contain all the necessary IG clauses regarding Data Protection and Freedom of Information	Yes	Yes, all different contract templates used, but all have confidentiality and IG clauses in place. If no, please give reasons:				
32	Will the data be sent outside the European Economic Area (EEA)?	No	If yes, list countries involved				
33	Are procedures in place to prevent processing for direct marketing?	Yes	As per approvals, data is required to be kept confidential and collected/used only for the purposes of informing the research project outcomes. It cannot be or shared elsewhere. If no, how is it prevented:				
34	Is there any other information we need to be aware of?						

TECHNOLOGY:				STATUS				
				High	Significant	Moderate	Low	Insignificant
35	Descr be the technical configuration of the system/project/process *(include support & administration, tracking technologies, database structures such as SQL, security by design measures such as redundancy, single points of failure, back up)*	Personal data will be held on MS Excel spreadsheets (password protected) on NSFT IT shared folders only. For some studies, personal data is also shared via online portals (PROSPERO, REDCAP, REDPILL) which are based within Clinical Trial Units at universities, and are validated research database systems for the purposes of sharing research information only.						
36	Descr be the security measures that have been put in place (or will be in place) to secure access to and limit the use of the data *(such as username and password, smartcard, locked filing cabinets/room, restricted access to network files)*	Password protection of spreadsheets on NSFT shared folders only. The Sheet is located on a protected Trust drive, where only people signed off as being part of the NSFT research delivery team have access to the sheet (or indeed, any of the other documents on that drive!). No external people or those not working in the specific team (even under other areas of the same department) have access to the drive or any of its contents. All IT requests go through [redacted] only for approval, so I can regulate who has access to what and why they need it. Paper-based forms (i.e. signed consent forms and the research data) are held in locked cabinets in research offices. Online data portals are only accessible by trained research staff members working on those specific studies.						
37	If new technology, does it employ approved encryption standards for data at rest or in transit? *E.g. 256bit AES encryption*	Unknown	If yes, give details of secure platforms used This information will be confirmed when the research project is being considered					
			If no, give details of other encryption standards used					
38	If new technology does it share a commonly recognised secure platform? *E.g. Office 365, Microsoft SharePoint, encrypted email*	Unknown	If yes, give details of secure platforms used This information will be confirmed when the research project is being considered					
39	If new technology, might it be perceived as intrusive to privacy? *(facial recognition or biometrics)*	Unknown	If yes, give details: This information will be confirmed when the research project is being considered					
40	Are there any technical concerns that warrant further follow up?	Unknown	If yes, explain further This information will be confirmed when the research project is being considered					
41	Does the system/project/process have an audit trail?	Unknown	If Yes, how long are audit trails kept and how are they accessed: This information will be confirmed when the research project is being considered					
			If no, explain how the systems are audited:					

42	Is this software/technology or similar already is use within the organisation?	Unknown	If yes, give details of the technology involved and is the soft hosted on local or external servers This information will be confirmed when the research project is being considered					
43	Who will be the Information Asset Owner (IAO) and Asset Administration(s)? *(name, job title and contact details)*	Information Asset Owner (IAO): This information will be confirmed when the research project is being considered						
		Information Asset Administrator(s): This information will be confirmed when the research project is being considered						
44	Is there a Business Continuity Plan (BCP) in place for the system/project/process	Unknown	If yes, list BCP Ref. Number: This information will be confirmed when the research project is being considered					
			If no, why not and should we have one:					
45	Is there a Disaster Recovery Plan (DRP) in place for the system/project/process	Unknown	If yes, list DR Ref. Number: This information will be confirmed when the research project is being considered					
			If no, why not and should we have one:					
46	Is the data being retrieved by a personal identifier *e.g. RMY Number, NHS Number, NI number)*	No	If yes, give details:					
			In no, how is it being retrieved: Pseudonymised Participant ID provided for research study.					
47	Will formal staff training be required before accessing the data?	Yes	If yes, give details of what is required and numbers: All staff are provided training by the sponsor/data controller.					
48	Does the system/project/process involve pulling together information about people from difference places, linking it, cross-referencing?	Unknown	If yes, give details: This information will be confirmed when the research project is being considered					
49	Is there any other information we need to be aware of?							

IDENTIFIED RISKS

Information Governance section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name/Job Title):	[redacted]

Information Security Section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name/Job Title):	[redacted]

The following risks have been identified and are to be managed in accordance with the Trust's Risk Management Strategy.

IMPORTANT: The Data Protection Officer and/or the Senior Information Risk Officer are required to review/approve the DPIA, subject to the identified risks being mitigated.

RECOMMENDATIONS AND RISKS		
It is recommended that: *Select as appropriate*	An Information Sharing Agreement is created	☐
	The DPO/SIRO accepts these recommendations and risks and permits the processing to proceed	☑
	The DPO/SIRO DOES NOT permit the processing as described. This would be subject to further mitigation of the HIGH RISKS	☐

Additional Comments

An Information Sharing Agreement is not required to be created from this DPIA. This DPIA covers the processes and procedures used when
Where questions on both the IG - General and IG - Security Tabs have been answered as 'Possible' or 'Unknown' this information will be confirmed
Attached are the following documents:

1. List of research projects undertaken since GDPR went live
2. Full Dataset Trial Form
3. Sealed Envelope User Guide

APPROVAL-DATA PROTECTION OFFICER		
As Data Protection Officer, I confirm that the highest level of risk identified in this DPIA is:	Low	
Processing may commence. The risks are proportionate and they can be managed accordingly.		☑
Processing MUST NOT commence. Further mitigating actions are required.		☐
Additional Comments	**None**	
Name	**Richard Green Data Protection Officer**	
Signed/email date	**11-Oct-19**	

APPROVAL-SENIOR INFORMATION RISK OWNER		
As Senior Information Risk Owner, I confirm that the highest level of risk identified in this DPIA is:		
Processing may commence. The risks are proportionate and they can be managed accordingly.		☐

Processing MUST NOT commence. Further mitigating actions are required.	☐
Additional Comments	
Name	
Signed/email date	

DATA & NSFT'S LAWFUL BASIS TO PROCESS

GDPR Article (Personal Data)

What is Personal Data?	Any information relating to an identified or identifiable natural person ('data subject')
What is an identifiable natural person?	One who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
What information can be an identifier?	Name, Identification number, Location data, Online identifiers (internet protocol (IP) addresses, cookie identifiers, radio frequency identification (RF D) tags, MAC addresses, Advertising Ds, Pixel tags, Account handles, Device fingerprints

Article 6 (1) (b)	Processing is necessary for a contact you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6 (1) (c)	Processing is necessary for us to comply with the law (not including contractual obligations)
Article 6 (1) (d)	Processing is necessary to protect someone's life
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

GDPR Article (Special Categories of Data)

What is Special Category Data?	Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade Union membership, Genetic Data/Biometric data, Health date, Sexual orientation

Article 9 (2) (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 and social security and social protection law
Article 9 (2) (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person
Article 9 (2) (f)	Processing is necessary for the establishment, exercise or defence of legal claims or courts acting in judicial capacity
Article 9 (2) (g)	Processing is necessary for reasons of substantial public interest
Article 9 (2) (h)	Processing is necessary for the purposes of preventive and 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
Article 9 (2) (i)	Processing is necessary for reasons of public interest in the area of public health or ensuring health standards of quality and safety of health care and of medicinal products or medical devices
Article9 (2) (j)	Processing is necessary for scientific or historical research purposes or statistical purposes

RISK ANALYSIS TOOL

PART 1 - RISK CONSEQUENCE GRADING

GRADES		OUTCOME/SEVERITY						
Grade	**Category**	**Safety**	**Quality**	**Statutory Duty**	**Information Governance**	**Service Continuity**	**Finance**	**Reputation**
A	**CATASTROPHIC**	Fatality/Fatalities	Totally unacceptable treatment or service	Multiple breaches in statutory study	Inevitable Data Privacy Breach	Permanent loss of service or facility	>£10M	National media coverage for 3 or more days
		Multiple Permanent injuries or irreversible health effects	Gross failure to meet national professional standards	Sustained failure to meet national professional standards	Processing must not commence or cease immediately	Catastrophic impact on the environment		Total loss of public confidence
		Impacts a large number of people	Ombudsman injury	Prosecution	Mitigating action or solution to unacceptable risk will be required			Questions in the House
			Inquest		Data Protection Officer must be involved			
					Individuals Affected: 1 000+			
					Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: Will identify individual (s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			

B	**MAJOR**	Permanent or long-term incapacity/ disability	Unacceptable treatment of service	Multiple breaches in statutory duty	High chance of Data Privacy being compromised	Loss of service or facility > 1 week	£1m - £10M	National media coverage for less than 3 days
		Length of hospital stay increased by > 15 days	Non-compliance with national standards	Intermittent failure to meet professional standards	Mitigating action or solution to unacceptable risk will be required	Moderate impact on the environment		Service well below public expectation
		> 14 days off work	Independent review	Improvement notices	Individuals Affected: 100-1,000			
			Critical report	Enforcement action	Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: High Possibility of identifying individual(s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
					Data Protection Officer must be involved			
C	**MODERATE**	Injury requiring professional intervention	Significantly reduced effectiveness of treatment of service	Failure to meet internal professional standards and/or national performance standards	Moderate chance of Data Privacy being compromised	Loss of service or facility > 1 day	£100K - £1M	Local media coverage
		RIDDOR reportable	Formal complaint (stage 2)	Civil action for negligence	Mitigating actions to be implemented to reduce risk to accepted level.	Moderate impact on the environment		Long-term reduction in public confidence
		Length of hospital stay increased by 4-15 days	Potential to go to independent review		Individuals Affected: 11-100			
		7-14 days off work			Reporting Requirements: Internal reporting and MAY need reporting to ICO			
					Sensitivity Factor: possibility of identifying individual (s)			
					Financial Penalty Risk: May lead to serious * fines from ICO			
					Data Protection Officer to be made aware			
D	**MINOR**	Minor injury dealt with one site (first aid)	Suboptimal overall treatment or service	Failure to meet internal professional standards	Minor chance of Data Privacy being compromised	Loss of service or facility > 8 hours	£5K to £100K	Local media coverage
		Length of hospital stay increased by 1 - 3 days	Formal complaint (stage 1)		Risk has been accepted or require minimal mitigating actions to rectify	Minor impact on the environment		Short-term reduction in public confidence
		Under 7 days off work	Local resolution		Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			
E	**INSIGNIFICANT**	Minimal injury requiring no treatment	Suboptimal peripheral treatment or service	Minor breach of internal professional standards	No/Low impact Risks to Data Privacy	Loss of service or facility <1 hour	<£5K	Rumours
			Informal complaint/inquiry		Identified Risks requiring no/minimal intervention	Minimal or no impact on the environment		Potential for public concern
					Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			

* The ICO will determine the fine based on a two-tiered sanction regime – lesser fines equate a max of €10 million or 2% of organization's global turnover.
** The ICO will determine the fine based on a two-tiered sanction regime – serious fines equate a max of €20 million or 4% of organization's global turnover.

PART 2 - RISK RATING MATRIX

To rate a risk

1
2 Grade the likelihood (Part 2)
3 Multiply this consequence (1-5) by the likelihood (1-6) to get the risk rating

		LIKELIHOOD				
		5	4	3	2	1
		Almost Certain	Likely	Possible	Unlikely	Rare
		Will undoubtedly happen, possible frequently	Will probably happen, but not persistently	Might happen occasionally	Not expected to happen, but could do so	May occur only in exceptional circumstances
CONSEQUENCE	5 Catastrophic	25	20	15	10	5
	4 Major	20	16	12	8	4
	3 Moderate	15	12	9	6	3
	2 Minor	10	8	6	4	2
	1 Insignificant	5	4	3	2	1

PART 3 - RISK MANAGEMENT - ACTION AND TIMESCALES

Risk Level	Action and Timescales
HIGH 15 - 25	Immediate action must be taken to manage and mitigate the risk. Control measures should be put into place to reduce the consequence of the risk or the likelihood of it occurring. A number of control measures may be required and significant resources may have to be allocated to reduce the risk.
SIGNIFICANT 8 - 12	Efforts should be made to reduce the risk but the cost of prevention should be measured and weighed against the consequence of the risk. Establish more precisely the likelihood of harm as a basis for determining the need for improved controls.
MODERATE 4 - 6	The likelihood of harm should be established before implementing further controls. Existing controls should be monitored and consideration should be given to a more cost-effective solution that imposes no additional cost.
LOW 1 - 3	Acceptable risk, no further action or additional controls are required. A risk at this level should be monitored, and reassessed at appropriate internals to ensure that it has not worsened.

Risk Analysis Tool taken from Q18 - Risk Management Strategy - Version 05 - dated 23rd March 2018

IG-DPIA NO:	DPIA-129	**IGT TSK NO:**	IGT-122637
ISA NO:	ISA-135	**IGT TSK NO:**	IGT-124385

INDEX			
Tab 1	Introduction		
Tab 2	Information Governance - General (Q1 to Q34)		
Tab 3	Information Governance - Security (Q35 to Q49)		
Tab 4	Identified Risks		
Tab 5	Recommendations & Signatures		
Tab 6	Reference Tab		

IG-DPIA NO:	DPIA-129	**IGT TSK NO:**	IGT-122637
ISA NO:	ISA-135	**IGT TSK NO:**	IGT-124385

DATA PROTECTION IMPACT ASSESSMENT

Under GDPR, it is now a legal requirement that a Data Protection Impact Assessment (DPIA) is completed at the start of ALL projects (major and minor) involving the use of personal data or significant changes are being made to an existing process or project. ALL final outcomes should be integrated back into the project and process.

This tool must be completed if there is a change to an existing service/technology or a new process/technology or service that could involve a new use or significant changes to how personal data is handled or processed.

Title of Project / Process:	Wellbeing Step 2 referrals to ICS Digital Therapies	
New DPIA	Yes	If no, insert previous DPIA number:
Customers/Stakeholders *(Full name(s), department(s) and contact details of all Customers/Stakeholders)*	[redacted]	
Project Lead: *(Full name, job title and contact details)*	[redacted]	
Proposed start date for the project or processing to commence	Date: April 2019	
If project or processing of data has already commenced, please give your reasons for not previously completed a DPIA (formerly called Privacy Impact Assessment).	This was brought to the attention of IG by Contracts in late May	
DPIA Conducted by:	[redacted]	[redacted]

SUMMARY OF THE PROJECT/PROCESS **Please give a brief summary of:**	
What is the purpose of the project?	Provision of IAPT specific therapy and treatments to patients in the care of Wellbeing - patients in question will be on their Step 2 IAPT Waiting List. A contract has been drawn up between ICS Digital Therapies and Wellbeing for outsourcing of IAPT therapy services - this will reduce pressure on the service, reduce the number of patients waiting for therapy, generally improve access to services, and ensure that patients are getting the help they need in a timely fashion. As per the contract with ICS patients on the waiting list will be referred to them via IAPTus by Wellbeing. The sharing of this information via the patient's IAPTus record will enable ICS to provide a remote / digital psychological therapy service to them up to the IAPT recommended maximum of 6 sessions. The service patients receive from ICS will be the same type of treatment that they would otherwise receive from Wellbeing. N.B. There are currently talks to extend the contract between ICS and Wellbeing with a contract variation - this will faciliate the referral of Wellbeing patients identified as suitable to receive treatment from ICS as part of a 'business as usual' (BAU) approach regarding the provision of treatment to their Step 2 patients.
What the project aims to achieve?	Outsourcing provision for Wellbeing Step 2 patients will reduce pressure on the service, reduce the number of patients waiting for therapy, generally improve access to services and ensure that patients are getting the help they need in a timely fashion.
What are the benefits provided by the project?	Outsourcing the provision will reduce pressure on the Wellbeing service, reduce the number of patients waiting for therapy, generally improve access to services and ensure that patients are getting the help they need in a timely fashion. This remote, modernised style of treatment also improves access for patients who would not normally be able to attend CBT appointments during 'normal working hours' - appointments can be scheduled with more emphasis on the patient's convenience and availability, and the therapy sessions will be conducted on the phone or via the video and messaging platform 'Fuze'.
What is the intended effect on individuals?	Provision of IAPT specific remote/digital based therapy treatment to Step 2 Wellbeing patients
What is the nature of your relationship with the individuals?	Wellbeing patients on Step 2 IAPT

How much control will the individuals have over the project/process?	Patients will be on IAPT Step 2 - should they not wish to engage with ICS they can theoretically object, however it would not be in their best interest as this is essentially the same type of treatment they would receive directly from Wellbeing. Some of these patients will have already been waiting for CBT / therapy services and treatment.
Will this project/process include dealing with children or other vulnerable groups?	No, patients will be over the age of 18. Dependent on circumstances some may be vulnerable however, as the patients on the Step 2 waiting list will have been identified with mild to moderate symptoms of depression and anxiety
What type of processing does it involve?	As per contract and proposed variations to follow. Wellbeing Step 2 patients will be referred to ICS Digital Therapies via IAPTus for the provision of remote and digital therapy services - this will either be as part of a waiting list reduction or in line with a contracted BAU referral process as established between the two parties. ICS staff will contact patients within 2 days to arrange an appointment Relevant webform questionnaires will be sent to service user via patient IAPTus portal before the appointment. Treatment sessions will be conducted via Fuze platform or on the phone as arranged with the patient, and assessment and IAPT MDS info will be recorded on the patient's IAPTus record which will be accessible to Wellbeing staff, and notes recorded in the clinical contact section will be available within 24 hours of the appointment. If the Therapist feels that a patient at risk, the ICS Supervisor / Clinical Lead will contact NSFT Wellbeing to discuss the appropriate actions necessary. In addition Wellbeing will receive reporting information from ICS on a weekly basis; this will include number of referrals received, timescales, appointment information (offered, attended, DNA) and recovery rate

INFORMATION GOVERNANCE:						STATUS			
						High	Significant	Moderate	Low
1	What is the nature of the data and does this include special category or criminal offence(including alledged offences) data? *(Please select all those appropriate)*	Personal ☑	Special Category ☑	Criminal Offence ☐	Corporate Sensitive ☐				
		Information as per IAPTus referral - this includes special category and personal identifiable data Patient name and contact details NHS number Questionnaires and assessment scores Reporting information - referrals received, time from referral to treatment, appointment data (offered, attended, DNA) and recovery rate GP Details N.B. a minimum dataset (MDS) is included in the Information Sharing Agreement - this covers a full IAPTus referral which are the defined access and processing restrictions							
2	What is the source of the data? *(Please select all those appropriate)*	Patient ☑	Staff ☑	Other ☐					
		Personal, special category and healthcare information from patient and staff as recorded on the NSFT IAPTus record will be shared with ICS as per the service contract - information added to the patient's IAPTus care record from this point onwards will be from the patient and the relevant PWP / CBT Therapist at ICS							
3	Describe how the system/project/process will collect personal data, special category data or corporately sensitive data that has not been collected before?	Patient personal and special category information will not be collected in a way that it has not been before, this is just an outsourcing of provision to ensure patients on Step 2 are getting the help they need in a timely fashion. Method of delivery may differ slightly from the way in which the treatment is provided by Wellbeing, but the CBT therapy itself will be based on IAPT evidence-based guidelines							
4	Is the information being used for a different purpose to currently being used?	No	No, the provision of the CBT therapy is just being outsourced and differs slightly in the method of delivery						
5	Is the information collected likely to raise additional privacy concerns or expectations This is above and beyond the routine processing of special category date	No	If yes, please give details Wellbeing will tell the patients before they are referred to ICS, this sharing of information will also be covered by our Trust-wide privacy notice as it is in the interest of care provision						

6	Will the project require you to contact individuals in ways which they may find intrusive?	No	If yes, please give details Patients will be made aware of the therapy service provided by ICS and the fact that they are being referred to them for treatment by the Wellbeing Service. Some will be on a waiting list with Wellbeing for this type of treatment anyway so are unlikely to find the contact from intrusive.					
7	Does the system/project/process results in decisions being made, or action being taken, against individuals in ways which can have a significant impact on them *Where fully automated decision making is involved this is to be treated as a SIGNIFICANT risk*	Decisions made ☑	Actions taken ☑	Significant impact ☐				
		No automated processing - Step 2 IAPT patients will be referred to ICS via IAPTus by Wellbeing staff, ICS will then contact them in the interest of providing CBT therapy sessions which they will likely already have been waiting for						
8	Describe the checks that have been carried out regarding adequacy, relevance and necessity for the collection of personal and sensitive data for this system/project/process?	A fully defined IAPT MDS is attached to the ISA - processing and access to the patient's information will be restricted to this via their IAPTus record. This is the same information that the Wellbeing service would be processing were they delivering the treatment and it is a standard IAPT data set which the system is designed to record. ICS will also provide additional reporting information to Wellbeing on a weekly basis; this will include number of referrals received, timescales, appointment information (offered, attended, DNA) and recovery rate.						
9	Any other information we need to be aware of?							

Initial Screening DPIA
Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO approval

ACCESSING DATA

10	Is access required to internal or external systems? *Please select all which apply*	Internal						
		Patients will be referred to ICS via IAPTus referral - ICS have a partnership with Mayden and have access to their own instance of the system, so no access needed to NSFT systems and vice versa. Data will however will be transferred from the NSFT instance of IAPTus to ICS in a two-way sharing process as per our service contract with them.						
11	Describe the authorisation process if accessing an external system	No external access - Wellbeing patients on Step 2 will be referred to ICS via direct IAPTus referral						
		Read Only: ☐	Modify: ☑	Full Control: ☑	Other: ☐			

12	What level of access will be authorised to the system/process/project?	When the personal and healthcare data of a patient is transferred from NSFT to ICS via IAPTus referral, their appointed staff's access to data will be in line with their organisational system access and security policies. The IAPTus system uses a role-based access model and as per ICS' Data Protection Policy (Q34) staff access to the data in this system will be on a need-to-know basis for the purpose of service provision, this being in line with the contract. These staff will have IG / DP training and attend regular security briefs in line with section 10.5 of aforementioned policy. NSFT IT / Systems Support and Wellbeing will have the ability to monitor access to records within IAPTus for every patient that is referred to ICS, via the 'User Activity' function.				
13	Describe how the access to data will be managed Please explain in full detail	Any referrals made via IAPTus to ICS will be from Wellbeing staff - prior to this there will be no legitimate relationship with the patient and ICS would not have access to the patient's data. IAPTus uses a role-based access model and access to the data at ICS will be based on their organisational access and security policies - this being in line their Data Protection Policy (Q34) and more specifically section 10.5 of said policy. Wellbeing and NSFT IT / Systems Support will have the facility to monitor ICS' access to a patient's records using the 'User Activity' function in IAPTus				
14	Who will create the accounts? *Please give full details of name/job title/area/department/organisation if not NSFT*	ICS staff will have their own access credentials for IAPTus because they already use the system, this will be managed by ICS' IT Department				
15	Who will be accessing the system/project/ process? *Please give details of name, job title, dept /service, location and number of people requiring access*	Data in IAPTus will be accessed by ICS staff on a need to know basis for the purpose of care / service provision in line with the contract and in adherence to their Data Protection policy (Q34) which states '*access to information is provided based on a "need to know" basis*.' Upon querying this with ICS I was advised by S.F. (one of their Senior Bid and Contract Managers) that '*only those people within ICS Digital Therapies that need to access data to deliver the service will do so. All data security is assured through strict information governance provisions, backed up by our accreditation with ISO27001. I understand that personal data is passed by the Trust, using their own IAPTus system, to refer a patient to ICS Digital Therapies. Patient data for the purpose of referral only is then received into our own IAPTus system. Patient data is then accessed and used to deliver the required service (assessment/treatment etc.) and on discharge, the same process happens in reverse* In line with the Service Specification, all assessments and treatment will be provided by a fully qualified PWP or CBT Therapist with supervision from a CBT supervisor / Clinical Lead. It is likely some non-clinical staff will have access to the data for the purposes of updating clinical notes and performing admin.				
16	Is there any other information we need to be aware of?					

RETENTION AND DISPOSAL OF DATA

17	What geographical area does the data cover?	Both Norfolk & Waveney and Suffolk Wellbeing service users					
18	Describe how long the data will be kept and how it will be stored	Summary of retention and disposal as per ISA Section 8 'Data Retention and Deletion':- 8.1 - data shall not be retained longer than necessary to fulfil agreed purposes (i.e. provision of care in line with the contract). 8.2 - outside of clause 8.1 data will be retained in line with applicable statutory / professional retention periods for the health and wellbeing industry (this would be in reference to the Records Management Code of Practice for HSC 2016 and at the end of the episode of care we would have responsibility for retention as the Data Controller). 8.3 and 8.4 - data will be destroyed on termination / expiry of the contract, on request of NSFT, or once retention is no longer necessary for the purposes of service provision (i.e. patient discharge). Upon discharge from ICS care the patient's data will be sent back to NSFT via IAPTus (we will have responsibility for retention as the Data Controller) and it will then be deleted from ICS data systems. Whilst necessary for the provision of service, all NSFT patient information provided to ICS will be stored in their IAPTus instance and their data systems in the UK. ICS are ISO27001 accredited and a specification of the minimum safeguards and security standards they apply to their systems can be found in their organisational Data Protection Policy (see Q34).					
19	Describe how the data will be disposed of	Patient information will be retained and disposed of as per ISA Section 8 'Data Retention and Deletion (see above) - patient personal data will flow back to NSFT on discharge from ICS care (will be available in NSFT instances of IAPTus). It should then be deleted from ICS systems as NSFT would have responsibility for retention as the data controller.					
20	Describe how the data will be transferred to a new service provider (if applicable)	Data will be transferred to ICS via IAPTus referral. All referrals to ICS will be managed by NSFT Wellbeing					
21	Will data be sent off site?	Yes	If yes, please give details - IAPTus ICS Digital Therapies are based in London and have confirmed that the data will remain in the UK, ISA also explicitly stipulates no processing outside the EEA.				
22	Describe the process of data portability for the system/project/process *Include information on plans in place regarding archiving/transferring/disposing of information should the system/project/process stop*	NSFT will have access to the information in IAPTus; ICS will delete the data when no longer needed as per ISA Section 8, however we will still have access in our IAPTus system.					

23	Is there any other information we need to be aware of?							

COMPLYING WITH THE LAW

24	Does this processing fall within our lawful reasons? *Please select all which apply*	Article 6 (1)	Article 9 (2)					
		b ☐	b ☐	h ☑				
		c ☐	c ☐	i ☐				
		d ☐	f ☐	j ☐				
		e ☑	g ☐					
		Legal basis for NSFT would be GDPR 6 (1) (e) for personal data and 9 (2) (h) for special category (direct care). As ICS are acting as a processor in line with an NHS sub-contract with us for the provision of CBT and therapy services, their legal basis for processing would also be 6 (1) (e) and 9 (2) (h).						
25	Will the data be shared with anyone who have not previously had reason to access it?	Yes						
		Due to the lack of a legitimate relationship ICS staff will not have previously had reason to access the data of NSFT patients referred to them, however they will have had access to the same data in relation to other patients in line with their contracts with other NHS Trusts and primary services. As we will be referring the patient to them for the provision of service in line with the sub-contract, this will establish a legitimate relationship for their staff to access their data where this is in the interest of providing care and in line with the terms of the ISA connected to this contract.						
26	Who are the Data Controllers and Data Processors	NSFT are data controller for data sent in IAPTus						
		ICS Digital Therapies are acting as a data processor as they are acting in line with a sub-contract to provide services CBT and therapy services to patients on our behalf						
27	Are the organisations registered with the ICO?	Yes	If yes, please give registration number: NSFT - Z5083441 [redacted]					

			In no, please give reasons:				
28	Do the organisations complete the DSP Toolkit?	Yes	If yes, please give registration number: ICS Group (ICSG Ltd) - 8J068 NSFT - RMY				
			In no, please give reasons:				
29	Are the organisations ISO 27001 certified?	Yes	If yes, please give registration number: ICS are accredited under certificate number 14128970 (validated by QMS)				
30	Describe the data security and protection requirements that have been defined between NSFT and the other controllers and processors	There is a contract between NSFT and ICS Digital Therapies to which an ISA is attached, this details the purposes and restrictions on the processing and the relevant security measures to be applied. Patient data for which NSFT are the controller will be shared with ICS within the IAPTus system, and on occasion minimal information (primarily IAPTus number) may be be exchanged by secure email in relation to a patient's care - this to be secured either by TLS connection (link has been proposed) or via Sophos SPX. Information sharing between the organisations will primarily be via IAPTus which is a secure platform with role-based access restriction. As per the ISA only those staff within ICS Digital Therapies that need to access the data as part of service provision will do so - this will be in line with their Data Protection Policy (see Q34) which also stipulates that they must have data protection / IG training and attend regular security awareness briefings. In line with this Data Protection Policy ICS and their systems have minimum standards and safeguards designed to ensure the security of confidential data and they are accredited with ISO27001 certification. As per the contract the patient's data will be transferred back to the Trust on discharge via IAPTus (NSFT will hold the retention responsibilties as the data controller); 'no personal data is retained for longer than the length of the sub-contract to enable the sub-contractor to carry out its obligations under this contract. Personal data is destroyed once processing of the personal data is no longer necessary for the purposes it was originally shared for'.					
31	Do the contracts contain all the necessary IG clauses regarding Data Protection and Freedom of Information	Yes	If yes - copy required				
			If no, please give reasons:				
32	Will the data be sent outside the European Economic Area (EEA)?	No	ISA stipulates no processing outside of the EEA and ICS have confirmed the data will be kept in the UK.				
33	Are procedures in place to prevent processing for direct marketing?	No	If yes, please give details: No legal basis for NSFT to process for direct marketing, as ICS are subcontracted by NSFT to provide CBT and therapy services they have confirmed no processing for direct marketing.				

			If no, how is it prevented:				
34	Is there any other information we need to be aware of?	ICS Data Protection Policy Feb 19					

			STATUS				
TECHNOLOGY:			High	Significant	Moderate	Low	Insignificant
35	Descr be the technical configuration of the system/project/process *(include support & administration, tracking technologies, database structures such as SQL, security by design measures such as redundancy, single points of failure, back up)*	Wellbeing Step 2 patients will be referred to ICS for CBT using the IAPTus system, this will involve an external data transfer from the Trust's instances of IAPTus to the instance run and managed by ICS. IAPTus has been developed by Mayden and data within the system is encrypted using the 256bit AES standard, access to the system will be managed and restricted by NSFT/ Wellbeing and ICS in line with their respective policies and procedures however the system uses a role-based access model. Backups and support for the core system are provided by Mayden as the developers and owners of the system, details can be found in the Trust BCP and DRP documents for IAPTus (IG8-30a & IG8-30b). Details about the minimum security safeguards and procedures that ICS apply to their technical and information systems can be found below at Q36. Further to a conversation with one of the Deputy Service Managers of the Wellbeing service, it seems some email communications may be necessary outside of the primary data exchange using IAPTus - I am told where this is necessary Wellbeing staff are currently following the Trust protocol of using Sophos SPX encyryption software to secure external communications with ICS that may contain confidential data. Following on from this conversation I have sent a proposal for the setup of a TLS link to our ICS BDM who has acted as my contact, this is still under review by them.					

36	Descr be the security measures that have been put in place (or will be in place) to secure access to and limit the use of the data *(such as username and password,smartcard, locked filing cabinets/room, restricted access to network files)*	IAPTus uses a role-based access model. The personal and healthcare data of a patient within the NSFT instances of IAPTus will be accessible to ICS only when that patient is referred to them which will also establish a legitimate relationship for them to access the data. Information about the security measures and procedures ICS have put in place to protect and restrict access to the data can be found in section 10.5 of their Data Protection policy (Q34):- *Information processed on ICSG systems shall be protected in accordance with the current published ICSG information security policies and procedures. For purposes of clarity, ICSG systems that are used to host, process, and store or transmit Sensitive Personal Data shall meet or exceed the following safeguards:* *• Systems shall be protected from unauthorised external access (firewalls)* *• System devices shall be protected by firewalls and anti-malware protection* *• Operating systems and applications shall be configured with latest security patches and updates* *• Data shall be backed up regularly and back-ups encrypted and stored in off-site location* *• Data should be securely removed before disposal of devices* *The following safeguards should be implemented to ensure the security of Sensitive Personal Data and Sensitive Medical Data on our systems:* *• Ensure that access to information is provided based on a "need to know" basis.* *• Passwords to devise accessing information meet or exceed published ICSG requirements* *• Hardcopy information is shredded when no longer required* *• Hardcopy information is stored in alarmed offices* *Additionally, the following safeguards should be implemented to ensure the security of Sensitive Medical Data:* *• Data must be encrypted when transmitted outside (off) of ICSG systems* *It should be noted that these minimum safeguards detailed herein apply to ICSG systems regardless of technology (wireless, software as a service, VoIP, virtualised or public, private or hybrid cloud computing etc.)* .							
37	If new technology, does it employ approved encryption standards for data at rest or in transit? *E.g. 256bit AES encrytption*	Yes	If yes, give details of secure platforms used IAPTus uses 256bit AES If no, give details of other encryption standards used					
38	If new technology does it share a commonly recognised secure platform? *E.g. Office 365, Microsoft SharePoint, encrypted email*	Yes	If yes, give details of secure platforms used IAPTus is used by a large proportion of IAPT services across the UK and is hosted by Mayden					
39	If new technology, might it be perceived as intrusive to privacy? *(facial recognition or biometrics)*	No	If yes, give details:					

40	Are there any technical concerns that warrant further follow up?	Yes	If yes,explain further As per Q35 - further to conversation with one of the DSMs of the Wel being service, some email communications may be necessary outside of the primary data exchange using IAPTus; currently using Sophos SPX encyryption software to secure any external communications with ICS that may contain confidential data. I have sent a proposal for the setup of a TLS link to ICS however this is still under review					
41	Does the system/project/process have an audit trail?	Yes	If Yes, how long are audit trails kept and how are they accessed: Audit trail will be present in IAPTus as upon discharge from ICS the patient's data will be sent back to NSFT instance. Even when the instance of care is closed the record will remain archived on our systems and those of Mayden. If no, explain how the systems are audited:					
42	Is this software/technology or similar already in use within the organisation?	Yes	If yes, give details of the technology involved and is the soft hosted on local or external servers IAPTus is already in use by the Trust, the software is hosted by Mayden on their servers in the UK. ICS also use IAPTus already.					
43	Who will be the Information Asset Owner (IAO) and Asset Administration(s)? *(name, job title and contact details)*	The IAO of data in the NSFT IAPTus systems will be the Service Managers of the Wellbeing service (likely [redacted]) IAAs would be their delegated Wellbeing staff processing / handling the data and making the referrals to ICS. As a data processor acting on behalf of NSFT (in line with our service contract with them) once referred to ICS via IAPTus system transmission, the relevant staff appointed by them to process and handle the data in the interest of care would also be acting as IAAs.						
44	Is there a Business Continuity Plan (BCP) in place for the system/project/process	Yes	If yes, list BCP Ref. Number: ICS have a general BCP in place for their key systems to enable their business processes to continue in the event of any service outages (see Q49) Additionally NSFT have a BCP for IAPTus (IG8-30a) which is the system that transfer of data between the service relies on If no, why not and should we have one:					
45	Is there a Disaster Recovery Plan (DRP) in place for the system/project/process	No	If yes, list DR Ref. Number: If no, why not and should we have one: ICS' BCP evidences some disaster recovery elements included in their continutity and recovery protocols (see Q49) NSFT also have a DRP for IAPTus (IG8-30b)					
46	Is the data being retrieved by a personal identifier *e.g. RMY Number, NHS Number, NI number)*	No	If yes, give details: In no, how is it being retrieved: Data is being shared via direct referral in the IAPTus system					

47	Will formal staff training be required before accessing the data?	No	ICS have a partnership with Mayden and provide their services to other NHS Trusts; appointed staff at ICS will be familiar with the use of IAPTus. Additionally, as per section 10.5 of their Data Protection Policy (Q34) - *All employees with access to ICSG systems that process the data that includes Sensitive Personal Data, shall be required to:* *• Receive data protection awareness training when being granted access; and* *• Receive regular security awareness briefings designed to heighten their information security awareness and remind them of their on-going security responsibilities*					
48	Does the system/project/process involve pulling together information about people from difference places, linking it, cross-referencing?	Yes	If yes, give details: Initial patient information will come from NSFT Wellbeing's instance of IAPTus which will be shared with ICS via direct referral. Information from this point will be recorded by ICS in their own instance of IAPTus, as part of their course of therapy with the patient; clinical contact notes, IAPT MDS, questionnaires and assessment information recorded by ICS will be made available to NSFT Wellbeing for patients they refer to them in IAPTus. Essentially there is a linked relationship between the NSFT Wellbeing and ICS instances of IAPTus for each patient they refer into their service on the system. This will ensure NSFT have access to updated care information for the patient.					
49	Is there any other information we need to be aware of?	ICS BCP and DRP 2018						
	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO aprroval							

IDENTIFIED RISKS

Information Governance section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name):	[redacted]

Information Security Section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name):	[redacted]

The following risks have been identified and are to be managed in accordance with the Trust's Risk Management Strategy.

IMPORTANT: The Data Protection Officer and/or the Senior Information Risk Officer are required to review/approve the DPIA, subject to the identified risks being mitigated.

PROCESSING MUST NOT COMMENCE UNTIL THESE RISKS ARER MITIGATED AT THE RIGHT LEVEL

Risk No	1			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

* **Consequence x impact = rating**
** **Consequence x impact = rating**

Risk No	2			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	3			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	4

Name of Risk					
Project Ref No					
Risk Owner					
Corporate Risk Reg No					
Risk Description					
Initial Risk*					
Target Risk*					
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised			
Other Risks		If yes, has the relevant area been advised			
*** Consequence x impact = rating** **** Consequence x impact = rating**					

Risk No	5				
Name of Risk					
Project Ref No					
Risk Owner					
Corporate Risk Reg No					
Risk Description					
Initial Risk*					
Target Risk*					
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised			
Other Risks		If yes, has the relevant area been advised			
*** Consequence x impact = rating** **** Consequence x impact = rating**					

RECOMMENDATIONS AND RISKS		
It is recommended that: *Select as appropriate*	An Information Sharing Agreement is created	☑
	The DPO/SIRO accepts these recommendations and risks and permits the processing to proceed	☐
	The DPO/SIRO DOES NOT permit the processing as described. This would be subject to further mitigation of the HIGH RISKS	☐

Additional Comments	A standard NHS sub-contract has been drafted by NSFT Contracts that will be put in place between NSFT and ICS Digital Therapies for the provision of this service	DRAFT NHSE Sub contract ICS Digital Therapies 2019-09-27
	An accompanying ISA has also been drafted and will be attached to this contract to facilitate the lawful and proportionate sharing of information in line with this service	DRAFT Data Sharing Agreement ICS Digital Therapies 14-10-19

APPROVAL-DATA PROTECTION OFFICER		
As Data Protection Officer, I confirm that the highest level of risk identified in this DPIA is:	Low	
Processing may commence. The risks are proportionate and they can be managed accordingly.		☑
Processing MUST NOT commence. Further mitigating actions are required.		☐
Additional Comments	**Nil**	
Name	**Richard Green**	
Signed/email date	**23-Oct-19**	

APPROVAL-SENIOR INFORMATION RISK OWNER		
As Senior Information Risk Owner, I confirm that the highest level of risk identified in this DPIA is:		
Processing may commence. The risks are proportionate and they can be managed accordingly.		☐

Processing MUST NOT commence. Further mitigating actions are required.	☐
Additional Comments	
Name	
Signed/email date	

DATA & NSFT'S LAWFUL BASIS TO PROCESS

GDPR Article (Personal Data)

What is Personal Data?	Any information relating to an identified or identifiable natural person ('data subject')
What is an identifiable natural person?	One who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
What information can be an identifier?	Name, Identification number, Location data, Online identifiers (internet protocol (IP) addresses, cookie identifiers, radio frequency identification (RF D) tags, MAC addresses, Advertising Ds, Pixel tags, Account handles, Device fingerprints

Article 6 (1) (b)	Processing is necessary for a contact you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6 (1) (c)	Processing is necessary for us to comply with the law (not including contractual obligations)
Article 6 (1) (d)	Processing is necessary to protect someone's life
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

GDPR Article (Special Categories of Data)

What is Special Category Data?	Racial or ethnic origin, Political opinions, Religious or phylosophical beliefts, Trade Union membership, Genetic Data/Biometric data, Health date, Sexual orientation

Article 9 (2) (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 and social security and social protection law
Article 9 (2) (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person
Article 9 (2) (f)	Processing is necessary for the establishment, exercise or defence of legal claims or courts acting in judicial capacity
Article 9 (2) (g)	Processing is necessary for reasons of substantial public interest
Article 9 (2) (h)	Processing is necessary for the purposes of preventive and 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
Article 9 (2) (i)	Processing is necessary for reasons of public interest in the area of public health or ensuring health standards of quality and safety of health care and of medicinal products or medical devices
Article9 (2) (j)	Processing is necessary for scientific or historical research purposes or statistical purposes

RISK ANALYSIS TOOL

PART 1 - RISK CONSEQUENCE GRADING

GRADES		OUTCOME/SEVERITY						
Grade	**Category**	**Safety**	**Quality**	**Statutory Duty**	**Information Governance**	**Service Continuity**	**Finance**	**Reputation**
A	**CATASTROPHIC**	Fatality/Fatalities	Totally unacceptable treatment or service	Multiple breaches in statutory study	Inevitable Data Privacy Breach	Permanent loss of service or facility	>£10M	National media coverage for 3 or more days
		Multiple Permanent injuries or irreversible health effects	Gross failure to meet national professional standards	Sustained failure to meet national professional standards	Processing must not commence or cease immediately	Catastrophic impact on the environment		Total loss of publc confidence
		Impacts a large number of people	Ombudsman injury	Prosecution	Mitigating action or solution to unacceptable risk will be required			Questions in the House
			Inquest		Data Protection Officer must be involved			
					Individuals Affected: 1 000+			
					Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: Will identify individual (s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			

B	**MAJOR**	Permanent or long-term incapacity/ disability	Unacceptable treatment of service	Multiple breaches in statutory duty	High chance of Data Privacy being compromised	Loss of service or facility > 1 week	£1m - £10M	National media coverage for less than 3 days
		Length of hospital stay increased by > 15 days	Non-compliance with national standards	Intermittent failure to meet professional standards	Mitigating action or solution to unacceptable risk will be required	Moderate impact on the environment		Service well below public expectation
		> 14 days off work	Independent review	Improvement notices	Individuals Affected: 100-1,000			
			Critical report	Enforcement action	Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: High Possibility of identifying individual(s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
					Data Protection Officer must be involved			
C	**MODERATE**	Injury requiring professional intervention	Significantly reduced effectiveness of treatment of service	Failure to meet internal professional standards and/or national performance standards	Moderate chance of Data Privacy being compromised	Loss of service or facility > 1 day	£100K - £1M	Local media coverage
		RIDDOR reportable	Formal complaint (stage 2)	Civil action for negligence	Mitigating actions to be implemented to reduce risk to accepted level.	Moderate impact on the environment		Long-term reduction in public confidence
		Length of hospital stay increased by 4-15 days	Potential to go to independent review		Individuals Affected: 11-100			
		7-14 days off work			Reporting Requirements: Internal reporting and MAY need reporting to ICO			
					Sensitivity Factor: possibility of identifying individual (s)			
					Financial Penalty Risk: May lead to serious * fines from ICO			
					Data Protection Officer to be made aware			
D	**MINOR**	Minor injury dealt with one site (first aid)	Suboptimal overal treatment or service	Failure to meet internal professional standards	Minor chance of Data Privacy being compromised	Loss of service or facility > 8 hours	£5K to £100K	Local media coverage
		Length of hospital stay increased by 1 - 3 days	Formal complaint (stage 1)		Risk has been accepted or require minimal mitigating actions to rectify	Minor impact on the environment		Short-term reduction in public confidence
		Under 7 days off work	Local resolution		Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			
E	**INSIGNIFICANT**	Minimal injury requiring no treatment	Suboptimal peripheral treatment or service	Minor breach of internal profesional standards	No/Low impact Risks to Data Privacy	Loss of service or facility <1 hour	<£5K	Rumours
			Informal complaint/inquiry		Identified Risks requiring no/minimal intervention	Minimal or no impact on the environment		Potential for public concern
					Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			

* The ICO will determine the fine based on a two-tiered sanction regime – lesser fines equate a max of €10 million or 2% of organization's global turnover.
** The ICO will determine the fine based on a two-tiered sanction regime – serious fines equate a max of €20 million or 4% of organization's global turnover.

PART 2 - RISK RATING MATRIX

To rate a risk

1
2 Grade the likelihood (Part 2)
3 Multiply this consequence (1-5) by the likelihood (1-6) to get the risk rating

		LIKELIHOOD				
		5	4	3	2	1
		Almost Certain	Likely	Possible	Unlikely	Rare
		Will undoubtedly happen, possible frequently	Will probably happen, but not persistently	Might happen occasionally	Not expected to happen, but could do so	May occur only in exceptional circumstances
CONSEQUENCE	5 Catastrophic	25	20	15	10	5
	4 Major	20	16	12	8	4
	3 Moderate	15	12	9	6	3
	2 Minor	10	8	6	4	2
	1 Insignificant	5	4	3	2	1

PART 3 - RISK MANAGEMENT - ACTION AND TIMESCALES

Risk Level	Action and Timescales
HIGH 15 - 25	Immediate action must be taken to manage and mitigate the risk. Control measures should be put into place to reduce the consequence of the risk or the liikelihood of it occurring. A number of control measures may be required and significant resources may have to be allocated to reduce the risk.
SIGNIFICANT 8 - 12	Efforts should be made to reduce the risk but the cost of prevention should be measured and weighed against the consequence of the risk. Establish more precisely the likelihood of harm as a basis for determining the need for improved controls.
MODERATE 4 - 6	The likelihood of harm should be established before implementing further controls. Existing controls should be monitored and consideration should be given to a more cost-effective solution that imposes no additional cost.
LOW 1 - 3	Acceptable risk, no further action or additional controls are required. A risk at this level should be monitored, and reassessed at appropriate internals to ensure that it has not worsened.

Risk Analysis Tool taken from Q18 - Risk Management Strategy - Version 05 - dated 23rd March 2018

IG-DPIA NO:	DPIA-165	**IGT TSK NO:**	IGT-117871
ISA NO:		**IGT TSK NO:**	

INDEX			
Tab 1	Introduction		
Tab 2	Information Governance - General (Q1 to Q34)		
Tab 3	Information Governance - Security (Q35 to Q49)		
Tab 4	Identified Risks		
Tab 5	Recommendations & Signatures		
Tab 6	Reference Tab		

IG-DPIA NO:	DPIA-165	**IGT TSK NO:**	IGT-117871
ISA NO:		**IGT TSK NO:**	

DATA PROTECTION IMPACT ASSESSMENT

Under GDPR, it is now a legal requirement that a Data Protection Impact Assessment (DPIA) is completed at the start of ALL projects (major and minor) involving the use of personal data or significant changes are being made to an existing process or project. ALL final outcomes should be integrated back into the project and process.

This tool must be completed if there is a change to an existing service/technology or a new process/technology or service that could involve a new use or significant changes to how personal data is handled or processed.

Title of Project / Process:	Voiceability / Total Voice Suffolk Advocacy Services and Avocet Ward		
New DPIA	Yes	If no, insert previous DPIA number: New	
Customers/Stakeholders *(Full name(s), department(s) and contact details of all Customers/Stakeholders)*	Name [redacted]	Dept: Avocet Ward (Woodlands)	Contact: [redacted]
Project Lead: *(Full name, job title and contact details)*	Name: [redacted]	[redacted]	[redacted]
Proposed start date for the project or processing to commence	N/A - as a provider of mental health services NSFT have engaged with advocates for some time and will continue to do so in line with legal obligations		
If project or processing of data has already commenced, please give your reasons for not previously completed a DPIA (formerly called Privacy Impact Assessment).	Was made aware of processing through query about proposed opt-out referral system (rejected on proportionality grounds). IG were already aware that the Trust engages with the advocates and the processing forms a part of legal / statutory obligation as well as access to these services being part of the criteria that is assessed by the CQC		
DPIA Conducted by:	Name: [redacted]	[redacted]	[redacted]

SUMMARY OF THE PROJECT/PROCESS

Please give a brief summary of:

What is the purpose of the project?	Access to advocacy services for service users in Avocet inpatient ward (Woodlands), more specifically where they may be eligible to a non-instructed advocate (NIA) under the Mental Health Act 1983, Mental Capacity Act 2005, or the Care Act 2014. Timely access to advocacy is also a CQC requirement that is inspected as part of the emphasis on ensuring the rights of service users. Matthew Jackson (CTL) raised a query with IG as the advocacy provider (Total Voice Suffolk / VoiceAbility) proposed an 'opt-out' referral system for all the ward's service users - it was suggested this would help ensure timely access to advocacy which is apparently an issue with service users having capacity issues. Further to advice from DPO this was deemed disproportionate as it would in essence mean NSFT sharing service user information with a non-healthcare organisation outside of vital interest, without a legitimate relationship, and without establishing lawful consent or any other legal basis for sharing it to begin within. Advice was given to Matthew on this basis verbally and this was followed up with a written confirmation of this advice the next day. Later followed up at which point Matthew confirmed he had circulated this advice to the team as well as the advocacy provider. IG were at this point copied in on an email from the Service manager of the advocacy service which attempted to challenge this advice; reference was made to ward staff having a legal duty to share where service users are eligible for NIA, as well as this being a part of 'a public task' conducted in line with an obligation to ensure the service users have access to advice / information about their section and their individual rights. No specific legislation or guidance was cited however. The opt-out system proposed would still be disproportionate however, so a response was sent on this basis. An offer was made to see if a viable ISA could be drawn up that ensured a consistent and assured approach to help with this issue, subject to a discussion and provision of some information of course. IG Services were also prepared to see if it would be viable to extend this agreement to cover all inpatient user wards, however due to no attempts to engage from Matthew or the Service Manager the ISA has now been scrapped. Current process is to obtain consent from service user or appointed carer / family with authority or log a best interest decision following a capacity assessment to facilitate lawful sharing of the service user's information for advocacy referral. Further information about standard referral process and normal operational procedures with advocates was received from the Charge Nurse based at Avocet - this has also been incorporated into the DPIA.
What the project aims to achieve?	Referrals for the provision of advocacy services - to ensure the ward staff and the Trust are fulfilling our statutory obligations and that any service users that may need or are entitled to the support of NIAs are receiving it in a timely fashion
What are the benefits provided by the project?	Provision of advocacy services satisfies a legal obligation to provide independent support and representation to eligible service users who may have capacity issues (following a capacity assessment), who are being detained, or are unable to be involved in making decisions about their care / have difficulty expressing their views, in particular this will be where a service user has nobody to actively help support and represent them. Advocates support service users through representation, helping them make their voice heard, and ensuring their rights are upheld and they can access the services and treatment they need.
What is the intended effect on individuals?	Provision of support through appointment of an independent representative to help ensure the service user's voice and concerns are being heard and addressed, that their legal rights are being upheld, and that they can access the services they need and are entitled to.
What is the nature of your relationship with the individuals?	NSFT service users in a ward setting - some will have capacity issues, and will have been detained under the MHA. Non-Instructed Advocates (NIAs) are appointed to independently represent the service users in line with CQC requirements and obligations under the Mental Health Act, Mental Capacity Act and the Care Act where service user is eligible

How much control will the individuals have over the project/process?	The main aims of advocacy are to ensure the service user's rights are upheld, they are being given access to the services they need and their voice is able to be expressed where they may have difficulty with this or they have nobody to actively support and represent their best interests. To this end the advocate will meet with the service user (this may be alongside a family member or carer as appropriate and may also include a staff member for security reasons) to discuss their care and provide assistance in voicing any concerns about patient's care or access to services, as well as helping to ensure they have an understanding of their rights and their entitlement to services and treatment. Access to advocacy is a statutory obligation where Service Users are elig ble under the Mental Health Act 1983, Mental Capacity Act 2005, or the Care Act 2014 - advocacy services falling into these categories are referred to as Non-Instructed Advocacy (NIA). Referrals to the advocates are dependant on capacity - in some cases the service user, following a capacity assessment, may not have capacity to give consent for their referral to an advocate (IMCA cases). Consent to refer will be sought where service users have capacity to provide informed lawful consent, however in some cases (where capacity may be an issue) this may be taken from their family or appointed representative with authority who may provide consent on their behalf in their best interest. If there is no such person a clinical decision of best interest will have to be made by respons ble ward and clinical staff which will be recorded in Lorenzo via a Best Interest Decision form and a Capacity Assessment.
Will this project/process include dealing with children or other vulnerable groups?	Avocet ward is an adult acute facility, so no children will be involved. Service users will be resident within an inpatient ward so can be considered vulnerable and additionally may also suffer from conditions that impair capacity.

What type of processing does it involve?	At present it is down to clinical staff to identify a service user's need for advocacy or eligibility for a Non-Instructed Advocate (NIA) – ideally this is discussed at the patient's admission review. Consent to refer the service users for advocacy will be sought where service users are able to provide lawful informed consent, however in cases where capacity is an issue this may have to be taken from their family, carer, or appointed representative who may provide consent on their behalf in their best interest should they have the authority to do so. If there is no such person or anyone with authority then following a capacity assessment a clinical decision of best interest will have to be made by respons ble ward and clinical staff; this will be recorded in Lorenzo via a Best Interest Decision form alongside the service user's Capacity Assessment. A referral for advocacy will then be sent to Total Voice / VoiceAbility via their professional referral form (Q9) which records information about the service user and the identity of the referrer. This is sent to Total Voice via the inbox xxxx@xxxxxxxxxxxxxxxx.xxx and is sent secured from NSFT using Sophos SPX encryption software. The form records personal and special category information to help highlight why the referral is needed and what the service user's needs are which would assist in identifying the type of advocacy required (i.e. IMCA, IMHA or Care Act). Some criminal offence information may possibly be included if pertinent to a risk involved with a particular patient. The advocates do not have access to any NSFT written or digital records, and they are not usually provided with clinical information other than what is necessary to maintain their safety until after they have met with a service user. Information may however be passed on to the advocate by the service user, their carer, or their family in meetings and communications with them, and this is at their own discretion. In cases where access to NSFT patient documentation is requested by the advocates this would be processed as a SAR by the NSFT Information Rights team in line with their procedures, however I have been advised by the Charge Nurse that she has not experienced any such requests other than for section papers which would be in line with an appeal to a MHA detention and these would be provided to the service user directly (or their family / representative) where appropriate. The advocate will meet with the service user (this may be alongside a family member or carer as appropriate and may also include a staff member for security reasons) to discuss their care and provide assistance in voicing any concerns about patient's care or access to services, as well as helping to ensure they have an understanding of their rights and their entitlement to services and treatment. Subsequent to this meeting the advocate may then approach clinical staff with any relevant questions that may have been raised by the service user or on their behalf.

INFORMATION GOVERNANCE:			STATUS				
			High	Significant	Moderate	Low	Insignificant
1	What is the nature of the data and does this include special category or criminal offence(including alleged offences) data? *(Please select all those appropriate)*	Personal ☑ | Special Category ☑ | Criminal Offence ☑ | Corporate Sensitive ☐ The advocates will receive information about the service user via the referral form (see Q9) - this records personal and special category information and will help highlight why the referral is needed and what the service user's needs are to assist in identifying the type of advocacy required (i.e. IMCA, IMHA or Care Act). Some criminal offence information may possibly be included if pertinent to a risk involved with a particular patient, as well as information for Equal Opportunities (optional). Aside from what is recorded in this form the advocates do not have access to any NSFT written or digital records on our service users, and they are not usually provided with clinical information other than what is necessary for referral and to maintain their safety until after they have met with a service user. Where there is an appeal to a MHA detention the advocates may request section papers but I have been advised by the Charge Nurse for Avocet these are provided to the service user (or their family) where appropriate. Following meeting with the service user (this may also include their family or carer as appropriate, as well as a member of staff for safety reasons) the advocate may then approach clinical staff with any relevant questions that may have been raised by the service user or on their behalf. Information may be passed on to the advocate by the service user, their carer, or their family in meetings and communications with the advocate (this is at their own discretion).				☑	
2	What is the source of the data? *(Please select all those appropriate)*	Patient ☑ | Staff ☑ | Other ☐ Information will come from staff and the service user's NSFT health record (i.e. Lorenzo). Service users will be discussed in a verbal context with the advocates by ward staff and additionally information may be passed on by the service user, their carer or their family in meetings and communications with the advocate - albeit at at their own discretion.				☑	
3	Describe how the system/project/process will collect personal data, special category data or corporately sensitive data that has not been collected before?	This process will not involve collecting personal, special category or any other type of confidential data in a way it has not been collected before, it is a simple referral process for providing service users with access to advocacy services.				☑	

4	Is the information being used for a different purpose to currently being used?	No	NSFT referring service users to advocacy services is not a new phenomenon					
5	Is the information collected likely to raise additional privacy concerns or expectations This is above and beyond the routine processing of special category date	No	Proposed opt-out referral system would likely have caused some privacy concerns alongside being disproportionate - IG have advised against this being implemented and this has been acknowledged					
6	Will the project require you to contact individuals in ways which they may find intrusive?	No	Consent to share the service user's personal information for advocacy referral will be sought where they have capacity to provide it - if this is not the case it may be sought from family / carer with authority on their behalf or a best interest decision may be made by staff following a capacity assessment. This process will ultimately be in their best interest as the advocate will meet with the service user, their carer, or their family to discuss their care etc and to help them voice any concerns they may have, as well as helping to ensure they have an understanding of their rights and entitlement to services and treatment.					
7	Does the system/project/process results in decisions being made, or action being taken, against individuals in ways which can have a significant impact on them *Where fully automated decision making is involved this is to be treated as a SIGNIFICANT risk*	Decisions made ☐	Actions taken ☐	Significant impact ☐				
		No automated processing, decision making or profiling. In reference to service users for whom capacity may be an issue, decisions will already have been made in the service user's best interest either by staff or their family, carer or authorised representative. Advocates' involvement with the service user can be statutory or voluntary dependent on circumstances of service user. The involvement of the advocates may result in actions being taken which have an impact on service users, however the role of the advocates is to support services users through representation, helping them make their voice heard, ensuring their rights are upheld and that they can access the services and treatment they need.							

8	Describe the checks that have been carried out regarding adequacy, relevance and necessity for the collection of personal and sensitive data for this system/project/process?	The advocates will receive basic information about the service user when they are referred to them which will highlight why the referral is needed and what the individual's needs are to assist in identifying the type of advocacy required (i.e. IMCA, IMHA or Care Act). This information will be shared via their referral form (Q9). Advocates are not usually provided with clinical information other than what is necessary to maintain their safety until after they have met with a service user. Following the meeting with the service user (may include their family or carer) the advocate may then approach clinical staff with any relevant questions that may have been raised by the service user or on their behalf Where there is an appeal the advocates may request section papers but I have been advised by the Charge Nurse for Avocet these are provided to the service user (or their family) where appropriate. In cases where access to NSFT patient documentation is requested and required by the advocates this would be processed as a SAR by the NSFT Information Rights team in line with their procedures, however I have been advised by the Charge Nurse that she has not experienced any such requests other than for section papers which would be in line with an appeal to a MHA detention and these would be provided to the service user directly (or their family / representative) where appropriate.					

9	Any other information we need to be aware of?	Based on assessment the legal bases for sharing are identified as follow:- 6 (1) (a) - service user is deemed to have capacity to consent to referral on their own, or where this is provided by a family member or appointed representative (i.e. carer) on their behalf and in their best interest. 6 (1) (c) - no ability to consent and the ward staff have identified advocacy need or they are eligible for statutory NIA under the MHA, MCA and Care Act. 9 (2) (a) - where service user is deemed to have capacity to consent to referral on their own, or where this is provided by a family member or appointed representative (i.e. carer) with authority on their behalf and in their best interest. 9 (2) (b) - The referral form collects information about protected characteristics for equal opportunities purposes, this is explained in their privacy notice: *'We may also ask for information related to your protected characteristics. Because we have to ask for this to fulfil the Equality Act (2010), our legal basis for processing this information is 'legal obligation'. This means we are obliged to ask you for the information. However, you can choose not to give it to us.'* 9 (2) (h) - VoiceAbility / Total Voice also cite this as their legal basis for processing healthcare data in their privacy notice: *'Some of the data that we hold may therefore include details about your health. This is a special category of data that requires an even greater level of protection. The additional basis on which we hold this data is that it is necessary for the provision of health or social care.'* Whilst the advocates will not be involved in the provision of health and social care, there is an argument that the advocates may influence a patient's care in their capacity of providing advice and representation, i.e. assisting with the expression of any concerns a service user may have, attempting to improve access to services they may need, and helping to ensure their rights are being upheld, such as checking they are being detained lawfully and assisting with appeals to detentions under the MHA etc.						
		This is a copy of VoiceAbility's privacy notice which has been adopted by the Total Voice Suffolk advocacy group of which they are the lead partner	VoiceAbility Privacy Notice					
		This is a copy of the referral form used by VoiceAbility / TVS for professional advocacy referrals	TVS Advocacy Professional Referral Form					

		~~information about how and why they handle, process, store, secure, retain and share the data~~ can be found in their comprehensive privacy notice (above) which includes a section specifically relating to data sent about a service user where making an advocacy referral in a professional capacity. As per this document '*Data that you submit verbally, either face-to-face or over the phone, by email, letter, paper form or online form is stored on our own secure case management system. The case management system uses encryption and password protection. It is not run on our own servers but operates on a cloud-based arrangement. It is held on Salesforce.com servers in the UK and EEA (specifically in Frankfurt and London).*' *'Some of your information may also be on email, especially if you submit it by email. Our emails are held on Microsoft's Office365 servers, the default locations for which are London, Cardiff and Durham. Our email system is encrypted and password protected.* *Salesforce and Microsoft have both signed up to EU rules regarding the moving of data outside of the UK and EEA.'* *'All of our staff are trained on how to keep your information safe.* *• In the case of information we have received on paper, we shred the physical paper after uploading to the case management system.* *• For digital records (including emails), after uploading a copy to the case management system, we delete any other copies or versions of the record that exists outside the case management system.'*					
	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO approval					

ACCESSING DATA										
10	Is access required to internal or external systems? *Please select all which apply*									
11	Describe the authorisation process if accessing an external system									
12	What level of access will be authorised to the system/process/project?	Read Only: ☐	Modify: ☐	Full Control: ☐	Other: ☐					

13	Describe how the access to data will be managed Please explain in full detail							
14	Who will create the accounts? *Please give full details of name/job title/area/department/organisation if not NSFT*							
15	Who will be accessing the system/project/ process? *Please give details of name, job title, dept /service, location and number of people requiring access*							
16	Is there any other information we need to be aware of?							

RETENTION AND DISPOSAL OF DATA								
17	What geographical area does the data cover?							
18	Describe how long the data will be kept and how it will be stored							
19	Describe how the data will be disposed of							
20	Describe how the data will be transferred to a new service provider (if applicable)							
21	Will data be sent off site?	Yes	If yes, please give details					

22	Describe the process of data portability for the system/project/process *Include information on plans in place regarding archiving/transferring/disposing of information should the system/project/process stop*							
23	Is there any other information we need to be aware of?							

COMPLYING WITH THE LAW										
24	Does this processing fall within our lawful reasons? *Please select all which apply*	Article 6 (1)	Article 9 (2)							
		b ☐	b ☐	h ☐						
		c ☐	c ☐	i ☐						
		d ☐	f ☐	j ☐						
		e ☐	g ☐							
25	Will the data be shared with anyone who have not previously had reason to access it?									
26	Who are the Data Controllers and Data Processors									
27	Are the organisations registered with the ICO?		If yes, please give registration number: In no, please give reasons:							

28	Do the organisations complete the DSP Toolkit?		If yes, please give registration number: In no, please give reasons:					
29	Are the organisations ISO 27001 certified?		If yes, please give registration number:					
30	Describe the data security and protection requirements that have been defined between NSFT and the other controllers and processors							
31	Do the contracts contain all the necessary IG clauses regarding Data Protection and Freedom of Information		If yes - copy required If no, please give reasons:					
32	Will the data be sent outside the European Economic Area (EEA)?		If yes, list countries involved					
33	Are procedures in place to prevent processing for direct marketing?		If yes, please give details: If no, how is it prevented:					
34	Is there any other information we need to be aware of?							

TECHNOLOGY:				STATUS				
				High	Significant	Moderate	Low	Insignificant
35	Descr be the technical configuration of the system/project/process *(include support & administration, tracking technologies, database structures such as SQL, security by design measures such as redundancy, single points of failure, back up)*	Referrals are sent to Total Voice via the inbox info@totalvoicesuffolk.org - email communications are sent secured from NSFT using Sophos SPX encryption software currently, however we are currently working to implement a TLS connection with TVS / VoiceAbility and this has been agreed upon by their Head of IT with whom I have discussed this proposition. Information about Total Voice systems taken from their privacy notice:- 'Data that you submit verbally, either face-to-face or over the phone, by email, letter, paper form or online form is stored on our own secure case management system. The case management system uses encryption and password protection. It is not run on our own servers but operates on a cloud-based arrangement. It is held on Salesforce.com servers in the UK and EEA [redacted] [redacted] Our email system is encrypted and password protected. Salesforce and Microsoft have both signed up to EU rules regarding the moving of data outside of the UK and EEA.'							
36	Descr be the security measures that have been put in place (or will be in place) to secure access to and limit the use of the data *(such as username and password, smartcard, locked filing cabinets/room, restricted access to network files)*	Voiceabilities email system is encrypted and password protected. Salesforce and Microsoft have both signed up to EU rules regarding the moving of data outside of the UK and EEA.'						
37	If new technology, does it employ approved encryption standards for data at rest or in transit? *E.g. 256bit AES encryption*	Yes	If yes, give details of secure platforms used 256bit AES If no, give details of other encryption standards used					
38	If new technology does it share a commonly recognised secure platform? *E.g. Office 365, Microsoft SharePoint, encrypted email*	Yes	If yes, give details of secure platforms used Office 365					
39	If new technology, might it be perceived as intrusive to privacy? *(facial recognition or biometrics)*	No	If yes, give details:					
40	Are there any technical concerns that warrant further follow up?	Yes	If yes, explain further:- Ensure a secure email connection is setup with Voiceability (TLS) this will ensure email between both parties is secure and does not require further encryption. [redacted]					

41	Does the system/project/process have an audit trail?	Yes	If Yes, how long are audit trails kept and how are they accessed: Audit for NSFT through Office 365 and Audits for Voiceability through their Office 365 as data controller. If no, explain how the systems are audited:					
42	Is this software/technology or similar already is use within the organisation?	Yes	If yes, give details of the technology involved and is the soft hosted on local or external servers Microsoft Office 365 UK hosted.					
43	Who will be the Information Asset Owner (IAO) and Asset Administration(s)? *(name, job title and contact details)*	Information Asset Owner would be Avocet ward manager - Matthew Jackson Asset administrators would be ward staff who send the referrals to the advocates - i.e. Juliette Calver, Avocet Charge Nurse						
44	Is there a Business Continuity Plan (BCP) in place for the system/project/process	Yes	If yes, list BCP Ref. Number:NSFT IG8-3a Microsoft Office 365 Exchange If no, why not and should we have one:					
45	Is there a Disaster Recovery Plan (DRP) in place for the system/project/process	Yes	If yes, list DR Ref. Number::NSFT IG8-3b Microsoft Offi ce 365 Exchange If no, why not and should we have one:					
46	Is the data being retrieved by a personal identifier *e.g. RMY Number, NHS Number, NI number)*	No	If yes, give details: In no, how is it being retrieved: Data shared by NSFT ward staff will come from them directly or will be retrieved from Lorenzo (patients will already be in the care of NSFT). Data will be recorded in the referral form (Q9) which will be sent to the advocates via secure email for the purpose of referral; this records identifiable data including patient name					
47	Will formal staff training be required before accessing the data?	No	If yes, give details of what is required and numbers:					
48	Does the system/project/process involve pulling together information about people from difference places, linking it, cross-referencing?	No	If yes, give details:					

49	Is there any other information we need to be aware of?	Referrals are sent to Total Voice via the inbox info@totalvoicesuffolk.org - email communications are sent secured from NSFT using Sophos SPX encryption software currently, however we are currently working to implement a TLS connection with TVS / VoiceAbility and this has been agreed upon by their Head of IT with whom I have discussed this proposition. Information about Total Voice systems taken from their privacy notice:- *'Data that you submit verbally, either face-to-face or over the phone, by email, letter, paper form or online form is stored on our own secure case management system. The case management system uses encryption and password protection. It is not run on our own servers but operates on a cloud-based arrangement. It is held on Salesforce.com servers in the UK and EEA* [redacted] *'Some of your information may also be on email, especially if you submit it by email. Our emails are held on Microsoft's Office365 servers, the default locations for which are* [redacted] *Our email system is encrypted and password protected.* *Salesforce and Microsoft have both signed up to EU rules regarding the moving of data outside of the UK and EEA.'*					
	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q49 (Tab 3) and sent for DPO approval						

IDENTIFIED RISKS

Information Governance section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name):	[redacted]

Information Security Section	
Have all the questions been answered satisfactory	Yes
Is further investigation required?	No
Completed by (Name):	[redacted]

The following risks have been identified and are to be managed in accordance with the Trust's Risk Management Strategy.

IMPORTANT: The Data Protection Officer and/or the Senior Information Risk Officer are required to review/approve the DPIA, subject to the identified risks being mitigated.

PROCESSING MUST NOT COMMENCE UNTIL THESE RISKS ARER MITIGATED AT THE RIGHT LEVEL

Risk No	1
Name of Risk	Proportionality of 'Opt-Out' Referral System proposed by Total Voice / Voiceability
Project Ref No	N/A
Risk Owner	[redacted] Avocet Ward
Corporate Risk Reg No	N/A

Risk Description	Query came from MJ (CTL for Avocet) who advised that the advocacy provider Total Voice Suffolk / VoiceAbility had proposed an 'opt-out' referral system for all the ward's service users. It was suggested this would help ensure timely access to advocacy which is apparently an issue with service users having capacity issues. Further to advice from DPO this was deemed disproportionate as it would in essence mean NSFT sharing service user information with a non-healthcare organisation outside of vital interest, without a legitimate relationship, and without establishing lawful consent or any other legal basis for sharing the service user's personal data to begin within. Advice was given to the CLT on this basis which was acknowledge and circulated to ward staff as well as the advocacy provider. The service manager of the advocacy service later queried this advice with the CLT and referenced ward staff having a legal duty to share where service users are eligible for NIA, as well as this being a part of 'a public task' conducted in line with an obligation to ensure the service users have access to advice / information about their section and their individual rights. No specific legislation or guidance was cited however. Ultimately the opt-out system proposed would still be disproportionate however, so a response was sent on this basis and an offer was made to discuss the possibility of an ISA with an alternative, more proportionate proposal. No response was received from the service manager however.			
Initial Risk*	12 (Moderate)			
Target Risk*	1-5 (Low)			
Clinical Risk	No	If yes, has the clinical safety officer/CCIO been advised		No
Other Risks	Yes	If yes, has the relevant area been advised		Yes - DPO and CTL
Mitigation: advice was given to internal staff and the external service manager to mitigate and prevent the risk becoming an issue, DPO was also notified and his advice sought. See Tab 2 Q5 and Tab 5 'Additional Comments' for more information.				
* **Consequence x impact = rating** ** **Consequence x impact = rating**				

Risk No	2
Name of Risk	
Project Ref No	
Risk Owner	
Corporate Risk Reg No	
Risk Description	
Initial Risk*	

Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	3			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	4
Name of Risk	
Project Ref No	
Risk Owner	
Corporate Risk Reg No	
Risk Description	
Initial Risk*	

Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

Risk No	5			
Name of Risk				
Project Ref No				
Risk Owner				
Corporate Risk Reg No				
Risk Description				
Initial Risk*				
Target Risk*				
Clinical Risk		If yes, has the clinical safety officer/CCIO been advised		
Other Risks		If yes, has the relevant area been advised		

***** **Consequence x impact = rating**
****** **Consequence x impact = rating**

RECOMMENDATIONS AND RISKS		
It is recommended that: *Select as appropriate*	An Information Sharing Agreement is created	☐
	The DPO/SIRO accepts these recommendations and risks and permits the processing to proceed	☑
	The DPO/SIRO DOES NOT permit the processing as described. This would be subject to further mitigation of the HIGH RISKS	☐

Additional Comments	An ISA was proposed between NSFT and Total Voice / VoiceAbility to both the CTL who raised the query and the Service Manager of Total Voice, however due to a lack of engagement from both the ISA has been scrapped following advice from DPO. Advice has been given by IG on the basis of the initial query, and I have received confirmation this has been acknowledged and cirulated to ward staff as well as the advocacy service to prevent the proposed 'opt-out' referral system on the grounds of proportionality. Although this was queried by the service manager of the advocates this was re-iterated as the proposal would still be disproportionate. Lawful consent or a legal basis for sharing will be established before any service users identified by ward staff that have a need for advocacy or eligibility for an NIA are referred to Total Voice. Follow-up with Charge Nurse on the process for referring service users to the advocates and the basis for their access to a service user's information has not indicated any other risks in need of mitigation.

APPROVAL-DATA PROTECTION OFFICER		
As Data Protection Officer, I confirm that the highest level of risk identified in this DPIA is:	Moderate	
Processing may commence. The risks are proportionate and they can be managed accordingly.		☑
Processing MUST NOT commence. Further mitigating actions are required.		☐
Additional Comments	The process whereby NSFT staff share the personal data of SU by default is to cease. SU should be made aware of the service and if they choose then their details may be shared.	
Name	**Richard Green DPO**	
Signed/email date	**19-Nov-19**	

APPROVAL-SENIOR INFORMATION RISK OWNER		
As Senior Information Risk Owner, I confirm that the highest level of risk identified in this DPIA is:		
Processing may commence. The risks are proportionate and they can be managed accordingly.		☐
Processing MUST NOT commence. Further mitigating actions are required.		☐
Additional Comments		
Name		
Signed/email date		

DATA & NSFT'S LAWFUL BASIS TO PROCESS

GDPR Article (Personal Data)

What is Personal Data?	Any information relating to an identified or identifiable natural person ('data subject')
What is an identifiable natural person?	One who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
What information can be an identifier?	Name, Identification number, Location data, Online identifiers (internet protocol (IP) addresses, cookie identifiers, radio frequency identification (RF D) tags, MAC addresses, Advertising Ds, Pixel tags, Account handles, Device fingerprints

Article 6 (1) (b)	Processing is necessary for a contact you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6 (1) (c)	Processing is necessary for us to comply with the law (not including contractual obligations)
Article 6 (1) (d)	Processing is necessary to protect someone's life
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

GDPR Article (Special Categories of Data)

What is Special Category Data?	Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade Union membership, Genetic Data/Biometric data, Health date, Sexual orientation

Article 9 (2) (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 and social security and social protection law
Article 9 (2) (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person
Article 9 (2) (f)	Processing is necessary for the establishment, exercise or defence of legal claims or courts acting in judicial capacity
Article 9 (2) (g)	Processing is necessary for reasons of substantial public interest
Article 9 (2) (h)	Processing is necessary for the purposes of preventive and 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
Article 9 (2) (i)	Processing is necessary for reasons of public interest in the area of public health or ensuring health standards of quality and safety of health care and of medicinal products or medical devices
Article9 (2) (j)	Processing is necessary for scientific or historical research purposes or statistical purposes

RISK ANALYSIS TOOL

PART 1 - RISK CONSEQUENCE GRADING

GRADES		OUTCOME/SEVERITY						
Grade	**Category**	**Safety**	**Quality**	**Statutory Duty**	**Information Governance**	**Service Continuity**	**Finance**	**Reputation**
A	**CATASTROPHIC**	Fatality/Fatalities	Totally unacceptable treatment or service	Multiple breaches in statutory study	Inevitable Data Privacy Breach	Permanent loss of service or facility	>£10M	National media coverage for 3 or more days
		Multiple Permanent injuries or irreversible health effects	Gross failure to meet national professional standards	Sustained failure to meet national professional standards	Processing must not commence or cease immediately	Catastrophic impact on the environment		Total loss of public confidence
		Impacts a large number of people	Ombudsman injury	Prosecution	Mitigating action or solution to unacceptable risk will be required			Questions in the House
			Inquest		Data Protection Officer must be involved			
					Individuals Affected: 1 000+			
					Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: Will identify individual (s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			

B	**MAJOR**	Permanent or long-term incapacity/ disability	Unacceptable treatment of service	Multiple breaches in statutory duty	High chance of Data Privacy being compromised	Loss of service or facility > 1 week	£1m - £10M	National media coverage for less than 3 days
		Length of hospital stay increased by > 15 days	Non-compliance with national standards	Intermittent failure to meet professional standards	Mitigating action or solution to unacceptable risk will be required	Moderate impact on the environment		Service well below public expectation
		> 14 days off work	Independent review	Improvement notices	Individuals Affected: 100-1,000			
			Critical report	Enforcement action	Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: High Possibility of identifying individual(s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
					Data Protection Officer must be involved			
C	**MODERATE**	Injury requiring professional intervention	Significantly reduced effectiveness of treatment of service	Failure to meet internal professional standards and/or national performance standards	Moderate chance of Data Privacy being compromised	Loss of service or facility > 1 day	£100K - £1M	Local media coverage
		RIDDOR reportable	Formal complaint (stage 2)	Civil action for negligence	Mitigating actions to be implemented to reduce risk to accepted level.	Moderate impact on the environment		Long-term reduction in public confidence
		Length of hospital stay increased by 4-15 days	Potential to go to independent review		Individuals Affected: 11-100			
		7-14 days off work			Reporting Requirements: Internal reporting and MAY need reporting to ICO			
					Sensitivity Factor: possibility of identifying individual (s)			
					Financial Penalty Risk: May lead to serious * fines from ICO			
					Data Protection Officer to be made aware			
D	**MINOR**	Minor injury dealt with one site (first aid)	Suboptimal overall treatment or service	Failure to meet internal professional standards	Minor chance of Data Privacy being compromised	Loss of service or facility > 8 hours	£5K to £100K	Local media coverage
		Length of hospital stay increased by 1 - 3 days	Formal complaint (stage 1)		Risk has been accepted or require minimal mitigating actions to rectify	Minor impact on the environment		Short-term reduction in public confidence
		Under 7 days off work	Local resolution		Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			
E	**INSIGNIFICANT**	Minimal injury requiring no treatment	Suboptimal peripheral treatment or service	Minor breach of internal professional standards	No/Low impact Risks to Data Privacy	Loss of service or facility <1 hour	<£5K	Rumours
			Informal complaint/inquiry		Identified Risks requiring no/minimal intervention	Minimal or no impact on the environment		Potential for public concern
					Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			

* The ICO will determine the fine based on a two-tiered sanction regime – lesser fines equate a max of €10 million or 2% of organization's global turnover.
** The ICO will determine the fine based on a two-tiered sanction regime – serious fines equate a max of €20 million or 4% of organization's global turnover.

PART 2 - RISK RATING MATRIX

To rate a risk

1 Grade the consequence (Part 1)
2 Grade the likelihood (Part 2)
3 Multiply this consequence (1-5) by the likelihood (1-6) to get the risk rating

		LIKELIHOOD				
		5	4	3	2	1
		Almost Certain	Likely	Possible	Unlikely	Rare
		Will undoubtedly happen, possible frequently	Will probably happen, but not persistently	Might happen occasionally	Not expected to happen, but could do so	May occur only in exceptional circumstances
CONSEQUENCE	5 Catastrophic	25	20	15	10	5
	4 Major	20	16	12	8	4
	3 Moderate	15	12	9	6	3
	2 Minor	10	8	6	4	2
	1 Insignificant	5	4	3	2	1

PART 3 - RISK MANAGEMENT - ACTION AND TIMESCALES

Risk Level	Action and Timescales
HIGH 15 - 25	Immediate action must be taken to manage and mitigate the risk. Control measures should be put into place to reduce the consequence of the risk or the likelihood of it occurring. A number of control measures may be required and significant resources may have to be allocated to reduce the risk.
SIGNIFICANT 8 - 12	Efforts should be made to reduce the risk but the cost of prevention should be measured and weighed against the consequence of the risk. Establish more precisely the likelihood of harm as a basis for determining the need for improved controls.
MODERATE 4 - 6	The likelihood of harm should be established before implementing further controls. Existing controls should be monitored and consideration should be given to a more cost-effective solution that imposes no additional cost.
LOW 1 - 3	Acceptable risk, no further action or additional controls are required. A risk at this level should be monitored, and reassessed at appropriate internals to ensure that it has not worsened.

Risk Analysis Tool taken from Q18 - Risk Management Strategy - Version 05 - dated 23rd March 2018

Norfolk and Suffolk
NHS Foundation Trust

Data Protection Impact Assessment

(By virtue of GDPR Article 35)

Title:	**Microsoft Forms for NSFT Surveys**		
DPIA Number:	DPIA-188	**IGT Task Number:**	IGT-141205
ISA NO:	N/A	**IGT Task Number:**	N/A

INDEX	
Tab 1	Introduction
Tab 2	Information Governance
Tab 3	Information Security
Tab 4	Identified Risks
Tab 5	Recommendations & Approvals
Tab 6	Reference Tab

DPIA Template Version: 4.1
Owner: DPO
Dated: Oct 19

DPIA Number:	DPIA-188	**IGT Number:**	IGT-141205
ISA Number:	N/A	**IGT Number:**	N/A

Data Protection Impact Assessment

Under GDPR, it is now a legal requirement that a Data Protection Impact Assessment (DPIA) is completed at the start of all projects (major and minor) involving the use of personal data or significant changes are being made to an existing services. The aim of the DPIA is to identifiy any risks to personal data that is being processed and feed that information back into the project.

Any risk that are identified should be managed in accordance with the Trust Risk Management Strategy.

The Data Protection Officer has the right to stop or prevent any processing where the risks are considered too high and exceed our risk appitite.

Title	**Microsoft Forms for NSFT Surveys**	
New DPIA:	Yes	If not, describe why DPIA is being done?
Customers/Stakeholders *(Full name(s), department(s) and contact details of all Customers/Stakeholders)*	[redacted]	
Project Lead *(Full name, job title and contact details)*	[redacted]	

Proposed start date for the project or processing to commence	TBC
If project or processing of data has already commenced, please give your reasons for not previously completing a DPIA (formerly called Privacy Impact Assessment)	N/A
DPIA Information Governance Lead	[redacted]
DPIA Information Securty Lead	

Summary of Project or Process	
Describe the project or process that this DPIA covers *Give a layman's overview of the project and state its aims, benefits.*	The Trust has used both the paid for and free vesions of Survey Monkey for conducting surveys within and outside of NSFT. Centralised accounts have been used which create information governance issues as users can view other survey responses as well as their own. Staff want an accessible, easy to use survey tool to create and manage their own surveys. Corporate Communications want a safe and secure tool for staff that they don't need to manage. An option has been put foward to use Microsoft Forms which comes as part of NSFTs procured Ofice 365 suite.
What is the intended effect on individuals?	Allow the Trust to facilitate surveys as required and get feed back on results. This will allow NSFT to use survey results to enhance Services, improve quality to name a few.
What is the nature of your relationship with the individuals?	Service User or Staff member.

How much control will the individuals have over the project/process?	It is up to the receiver of the survey to participate (no presure to take part).
Will this project/process include dealing with children or other vulnerable groups?	Dependant on the surveys being facilitated, but possibly could include these groups.
What type of processing does it involve?	Using the results of the surveys to produce analysis on different Trust services and functions.

INFORMATION GOVERNANCE						STATUS			
						High	Significant	Moderate	Low
1	What is the nature of the data and does this include special category or criminal offence(including alleged offences) data? *(Please select all those appropriate)*	Personal ☑	Special Category ☐	Criminal Offence ☐	Corporate Sensitive ☐				
2	What is the source of the data? *(Please select all those appropriate)*	Patient ☑	Staff ☑	Other ☑	If other describe below				
		Other external groups or 3rd parties that NSFT want to gain feedback from. Most surveys will involve NSFT Staff/Patients.							
3	Describe how the system/project/process will collect personal data, special category data or corporately sensitive data that has not been collected before?	The information collected will be via forms published on MS Teams and Intranet locations for staff to complete and on the website or via email for patients. Forms will request data pertaining to the requirements of the publisher of that form.							
4	Is the information being used for a different purpose to currently being used?	No	If yes, please give details						
5	Is the information collected likely to raise additional privacy concerns or expectations This is above and beyond the routine processing of special category date	No	If yes, please give details						
6	Will the project require you to contact individuals in ways which they may find intrusive?	No	If yes, please give details						
7	Does the system/project/process results in decisions being made, or action being taken, against individuals in ways which can have a significant impact on them *Where fully automated decision making is involved this is to be treated as a SIGNIFICANT risk*	Decisions made ☐	Actions taken ☐	Significant impact ☐	No ☑				
		This will just be routine surveys.							

8	Describe the checks that have been carried out regarding adequacy, relevance and necessity for the collection of personal and sensitive data for this system/project/process?	Checks will be conducted to ensure the surveys are to do with feedback on Service improvement they will be anonymous but if the person completing the Survey wishes to disclose their personal information e.g. Name, DOB, Address they do so by consent on submitting the form. Most surveys are anonymous for statistical purposes and may be used to guage satisfaction on overall system or service performance.						
9	What is the GDPR lawful basis for processing? *Please select all which apply*	Article 6 (1)	Article 9 (2)					
		a ☑	a ☐	g ☐				
		b ☐	b ☐	h ☐				
		c ☐	c ☐	i ☑				
		d ☐	d ☐	j ☑				
		e ☑	e ☐					
		f ☐	f ☐					
10	Any other information we need to be aware of?							
	Initial Screening DPIA Where Q1-10 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q10 (Tab 2) and Q48 (Tab 3) and sent for DPO approval							

ACCESSING DATA								
11	Is access required to internal or external systems? *Please select the appropriate option*							

12	Describe the authorisation process if accessing an external system					
13	Describe the access control model and its management?					
14	Who will create the accounts? *Please give full details of name/job title/area/department/organisation if not NSFT*					
16	Who will be accessing the system/project/ process?					
17	Is there any other information we need to be aware of?					

RETENTION AND DISPOSAL OF DATA						
18	Describe how long the data will be kept and how it will be stored					
19	Describe how the data will be disposed of					
20	At the transfer of a service, describe how the data will be transferred to or from another service provider (if applicable)					

21	Describe where is the data hosted? on-prem or cloud						
22	Describe the process of data portability for the system/project/process. *Include information on plans in place regarding archiving/transferring/disposing of information should the system/project/process stop*						
23	Is there any other information we need to be aware of?						

COMPLYING WITH THE LAW							
24	Will the data be shared with anyone who have not previously had reason to access it?		If yes, please give details				
25	Who are the Data Controllers and Data Processors?						
26	Describe the relationship between the Data Controllers and Data Processors.						
27	Are the organisations registered with the ICO?		If yes, please give registration number: In no, please give reasons:				
28	Do the organisations complete the DSP Toolkit?		If yes, please give registration number: In no, please give reasons:				

29	Are the organisations ISO 27001 certified?		If yes, please give registration number:				
31	Do the contracts contain all the necessary IG clauses regarding Data Protection and Freedom of Information?		If yes - copy required If no, please give reasons:				
32	Will the data be sent outside the UK?		If yes, list countries involved				
33	Are procedures in place to prevent processing for direct marketing?		If yes, please give details: If no, how is it prevented:				
34	Is there any other information we need to be aware of?						

INFORMATION SECURITY				STATUS				
				High	Significant	Moderate	Low	Insignificant
35	Describe the security by design measures and technical configuration. Consider: *Support & administration,* *Access Management* *Tracking technologies,* *Database structures, e.g. SQL,* *Redundancy,* *Single points of failure* *Back up* *Physical security*	Microsoft Forms is part of Microsoft Office 365 and allows users to create custom surveys, quizzes, polls, and questionnaires. It also can send an invitation to other users asking them to fill out the Microsoft Forms using a web browser on any device or computer. The creator can review the results in real time and can perform analysis on the collected data.						
36	If new technology, does it employ approved encryption standards for data at rest and in transit? e.*g. 256bit AES encryption*	Yes	If yes, give details of secure platforms used:-256bit AES If no, give details of other encryption standards used					
37	If new technology does it share a commonly recognised secure platform? e.*g. Office 365, Microsoft SharePoint*	Yes	If yes, give details of secure platforms used:-Office 365					
38	If new technology, might it be perceived as intrusive to privacy? *(facial recognition or biometrics)*	No	If yes, give details:					
39	Are there any technical concerns that warrant further follow up?	Yes	If yes, explain further:- Currently Forms is hosted in the United States and so not stored on UK data centres as per other Office 365 applications, it is understood that Microsoft will be looking to host forms at some point in the EEC/UK					
40	Does the system/project/process have an audit trail?	Yes	If Yes, how long are audit trails kept and how are they accessed: Office 365 have an extensive selection of audit tools which are accessible by administrators, these are currently stored as per the normal Microsoft contract (Infinitely) If no, explain how the systems are audited:					

41	Is this software/technology or similar already is use within the organisation?	Yes	If yes, give details of the technology involved and is the software hosted on local or external servers:- Office 365 which is hosted externally on Microsoft Azure servers.					
42	Who will be the Information Asset Owner (IAO) and Asset Administration(s)? *(name, job title and contact details)*	Lesley Barlow, Deputy Head of Communications						
43	Is there a Business Continuity Plan (BCP) in place for the system/project/process	No	If yes, list BCP Ref. Number: If no, why not and should we have one: Not required as non critical service.					
44	Is there a Disaster Recovery Plan (DR) in place for the system/project/process	No	If yes, list DR Ref. Number: Not required as non critical service. If no, why not and should we have one:					
45	Is the data being retrieved by a personal identifier *e.g. RMY Number, NHS Number, NI number*	No	If yes, give details: In no, how is it being retrieved:					
46	Will formal staff training be required before accessing the data?	No	If yes, give details of what is required and numbers:					
47	Does the system/project/process involve pulling together information about people from difference places, linking it, cross-referencing?	No	If yes, give details:					
48	Is there any other information we need to be aware of?	Staff will need to be given guidance on usage and the Trust communication Team will remain the primary contact and support for the process and surveys administered via Microsoft Forms. Currently Forms is hosted on the Office 365 platform based in the EEC Netherlands (NL) and not on UK data centres. Due to the system being hosted in the NL, it must not be used for confidential/sensitive data subject to future BREXIT agreement that need to be in place for data comming to the UK from the EEC. Surveys do not usually collect confidential information. Further information is available from the following Microsoft websiteFurther information is available from the following Microsoft website, https://forms.office.com/						

	Initial Screening DPIA Where Q1-9 has NOT identified any risks rated higher than LOW, then the DPIA may be summarised in Q9 (Tab 2) and Q48 (Tab 3) and sent for DPO approval					

ICT Risk register

IDENTIFIED RISKS

The following risks have been identified and are to be managed in accordance with the Trust's Risk Management Strategy.

IMPORTANT The Data Protection Officer and/or the Senior Information Risk Officer are required to review/approve the DPIA, subject to the identified risks being mitigated.

ID	Risk Reg ID	Name of risk	Risk Lead	Svs / Dept	Opened	Description of risk	INITIAL Conseq…	INITIAL Likeli…	INITIAL Rating	Controls in place	REVISED Conseq	REVISED Likeli	REVISED Rating	TARGET Conseq	TARGET Likeli	TARGET Rating
0	1453	Breach of Subject Access Request Confidentiality **EXAMPLE RISK PLEASE DELETE AFTER COMPLETION**	Richard Green	ICT Services **IF A CLINICAL RISK, INCLUDE AND INFORM CCIO**	30/04/2018	**Cause** If while responding to a Subject Access Request, Compliance team inadvertently disclosed third party information to unauthorised persons **Event** This lead to distress to a Service User **Effect** This may attract unwanted comment and publicity as well as leaving us liable to enforcement action from the Information Commissioner's Office	4	2	8	The Compliance Team's processes have been reviewed and improved to include double checks and management spot checks but there remains a latent risk of third party data being incorrectly disclosed, e.g. a handwritten phone number in 1000 page document. No further actions can be taken and this remains a risk that should be accepted.	3	2	6	1	2	2
1									0				0			0
2									0				0			0
3									0				0			0
4									0				0			0
5									0				0			0

RECOMMENDATIONS		
It is recommended that: *Select all as appropriate*	An Information Asset Owner be appointed for this activity	☐
	A new Information Sharing Agreement is created for this activity	☐
	An existing Information Sharing Agreement is in place and covers this activty	☐
	A new Business Continuity Plan is created for this activity	☐
	An existing Business Continuity Plan is updated for this activity	☐
	A new Distaster Recovery Plan is created for this activity	☐
	An existing Disaster Recovery Plan is updated for this activity	☐
	The DPO/SIRO accepts these recommendations, the risks and permits the processing to proceed	☑
	The DPO/SIRO does **NOT** permit the processing as described. This would be subject to further mitigation of the **SIGNIFICANT** and **HIGH** Risks	☐
Final Comments and Justifications	A more coperate and controlled [Administration/audit] system for performing staff surveys, quizes built around the Trusts current Microsoft Office 365 procured system. This solution also has no additional costs due to it being part of the Microsoft Office 365 system.	

APPROVAL- DATA PROTECTION OFFICER		
As DPO, I confirm that the highest level of risk identified in this DPIA is:	Low	
Processing may commence. The risks are proportionate and they can be managed accordingly.		☑
Processing MUST NOT commence. Further mitigating actions are required.		☐

Additional Comments	
Name	**Richard Green DPO**
Date	**19-Nov-19**

APPROVAL- SENIOR INFORMATION RISK OWNER	
As SIRO, I confirm that the highest level of risk identified in this DPIA is:	
Processing may commence. The risks are proportionate and they can be managed accordingly.	☐
Processing MUST NOT commence. Further mitigating actions are required.	☐
Additional Comments	
Name	
Date	

DATA & NSFT'S LAWFUL BASIS TO PROCESS

GDPR Article (Personal Data)

What is Personal Data?	Any information relating to an identified or identifiable natural person ('data subject')
What is an identifiable natural person?	One who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
What information can be an identifier?	Name, Identification number, Location data, Online identifiers (internet protocol (IP) addresses, cookie identifiers, radio frequency identification (RF D) tags, MAC addresses, Advertising IDs, Pixel tags, Account handles, Device fingerprints

Article 6 (1) (a)	The data subject has given consent to the processing of his or her personal data for one or more specific purposes
Article 6 (1) (b)	Processing is necessary for a contact you have with the individual, or because they have asked you to take specific steps before entering into a contract
Article 6 (1) (c)	Processing is necessary for us to comply with the law (not including contractual obligations)
Article 6 (1) (d)	Processing is necessary to protect someone's life
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 6 (1) (f)	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party

GDPR Article (Special Categories of Data)

What is Special Category Data?	Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade Union membership, Genetic Data/Biometric data, Health date, Sexual orientation

Article 9 (2) (a)	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
Article 9 (2) (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 and social security and social protection law
Article 9 (2) (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person
Article 9 (2) (d)	Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition
Article 9 (2) (e)	Processing relates to personal data which are manifestly made public by the data subject
Article 9 (2) (f)	Processing is necessary for the establishment, exercise or defence of legal claims or courts acting in judicial capacity
Article 9 (2) (g)	Processing is necessary for reasons of substantial public interest
Article 9 (2) (h)	Processing is necessary for the purposes of preventive and 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
Article 9 (2) (i)	Processing is necessary for reasons of public interest in the area of public health or ensuring health standards of quality and safety of health care and of medicinal products or medical devices
Article9 (2) (j)	Processing is necessary for scientific or historical research purposes or statistical purposes

RISK ANALYSIS TOOL

PART 1 - RISK CONSEQUENCE GRADING

GRADES		OUTCOME/SEVERITY						
Grade	**Category**	**Safety**	**Quality**	**Statutory Duty**	**Information Governance**	**Service Continuity**	**Finance**	**Reputation**
		Fatality/Fatalities	Totally unacceptable treatment or service	Multiple breaches in statutory study	Inevitable Data Privacy Breach	Permanent loss of service or facility	>£10M	National media coverage for 3 or more days
		Multiple Permanent injuries or irreversible health effects	Gross failure to meet national professional standards	Sustained failure to meet national professional standards	Processing must not commence or cease immediately	Catastrophic impact on the environment		Total loss of public confidence

5	**CATASTROPHIC**	Impacts a large number of people	Ombudsman injury	Prosecution	Mitigating action or solution to unacceptable risk will be required			Questions in the House
			Inquest		Data Protection Officer must be involved			
					Individuals Affected: 1,000+			
					Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: Will identify individual (s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
4	**MAJOR**	Permanent or long-term incapacity/ disability	Unacceptable treatment of service	Multiple breaches in statutory duty	High chance of Data Privacy being compromised	Loss of service or facility > 1 week	£1m - £10M	National media coverage for less than 3 days
		Length of hospital stay increased by > 15 days	Non-compliance with national standards	Intermittent failure to meet professional standards	Mitigating action or solution to unacceptable risk will be required	Moderate impact on the environment		Service well below public expectation
		> 14 days off work	Independent review	Improvement notices	Individuals Affected: 100-1,000			
			Critical report	Enforcement action	Reporting Requirements: Internal reporting and WILL need reporting to ICO			
					Sensitivity Factor: High Possibility of identifying individual(s)			
					Financial Penalty Risk: May lead to serious ** fines from ICO			
					Data Protection Officer must be involved			
3	**MODERATE**	Injury requiring professional intervention	Significantly reduced effectiveness of treatment of service	Failure to meet internal professional standards and/or national performance standards	Moderate chance of Data Privacy being compromised	Loss of service or facility > 1 day	£100K - £1M	Local media coverage
		RIDDOR reportable	Formal complaint (stage 2)	Civil action for negligence	Mitigating actions to be implemented to reduce risk to accepted level.	Moderate impact on the environment		Long-term reduction in public confidence
		Length of hospital stay increased by 4-15 days	Potential to go to independent review		Individuals Affected: 11-100			
		7-14 days off work			Reporting Requirements: Internal reporting and MAY need reporting to ICO			
					Sensitivity Factor: possibility of identifying individual (s)			
					Financial Penalty Risk: May lead to serious * fines from ICO			
					Data Protection Officer to be made aware			
2	**MINOR**	Minor injury dealt with one site (first aid)	Suboptimal overall treatment or service	Failure to meet internal professional standards	Minor chance of Data Privacy being compromised	Loss of service or facility > 8 hours	£5K to £100K	Local media coverage
		Length of hospital stay increased by 1 - 3 days	Formal complaint (stage 1)		Risk has been accepted or require minimal mitigating actions to rectify	Minor impact on the environment		Short-term reduction in public confidence
		Under 7 days off work	Local resolution		Individuals Affected: 1-11			

2	MINOR				Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			
1	INSIGNIFICANT	Minimal injury requiring no treatment	Suboptimal peripheral treatment or service	Minor breach of internal professional standards	No/Low impact Risks to Data Privacy	Loss of service or facility <1 hour	<£5K	Rumours
			Informal complaint/inquiry		Identified Risks requiring no/minimal intervention	Minimal or no impact on the environment		Potential for public concern
					Individuals Affected: 1-11			
					Reporting Requirements: Internal reporting only			
					Sensitivity Factor: Unlikely to identify individual (s)			
					Financial Penalty Risk: Unlikely			

* The ICO will determine the fine based on a two-tiered sanction regime – lesser fines equate a max of €10 million or 2% of organization's global turnover.
** The ICO will determine the fine based on a two-tiered sanction regime – serious fines equate a max of €20 million or 4% of organization's global turnover.

PART 2 - RISK RATING MATRIX

To rate a risk

1 Risk Consequence Grading (Part 1)
2 Grade the likelihood (Part 2)
3 Multiply this consequence (1-5) by the likelihood (1-5) to get the risk rating

		LIKELIHOOD				
		5	**4**	**3**	**2**	**1**
		Almost Certain	**Likely**	**Possible**	**Unlikely**	**Rare**
		Will undoubtedly happen, possible frequently	**Will probably happen, but not persistently**	**Might happen occasionally**	**Not expected to happen, but could do so**	**May occur only in exceptional circumstances**
CONSEQUENCE	**5 Catastrophic**	**25**	**20**	**15**	**10**	**5**
	4 Major	**20**	**16**	**12**	**8**	**4**
	3 Moderate	**15**	**12**	**9**	**6**	**3**
	2 Minor	**10**	**8**	**6**	**4**	**2**
	1 Insignificant	**5**	**4**	**3**	**2**	**1**

PART 3 - RISK MANAGEMENT - ACTION AND TIMESCALES

Risk Level	Action and Timescales
HIGH 15 - 25	Immediate action must be taken to manage and mitigate the risk. Control measures should be put into place to reduce the consequence of the risk or the likelihood of it occurring. A number of control measures may be required and significant resources may have to be allocated to reduce the risk.
SIGNIFICANT 8 - 12	Efforts should be made to reduce the risk but the cost of prevention should be measured and weighed against the consequence of the risk. Establish more precisely the likelihood of harm as a basis for determining the need for improved controls.
MODERATE 4 - 6	The likelihood of harm should be established before implementing further controls. Existing controls should be monitored and consideration should be given to a more cost-effective solution that imposes no additional cost.
LOW 1 - 3	Acceptable risk, no further action or additional controls are required. A risk at this level should be monitored, and reassessed at appropriate internals to ensure that it has not worsened.