

Privacy & Security Impact Assessment

Title	Ref number
<i>Trac Systems</i>	

DRAFT

PAGE							
ISSUE							
DATE							

PRIVACY & SECURITY IMPACT ASSESSMENT

Introduction

A Privacy & Security Impact Assessment enables GOSH to meet its legal/compliance obligations within the Data Protection Act 2018 and the General Data Protection Regulations 2016 (GDPR).

The Privacy & Security Impact Assessment ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to the Trust that risks are adequately managed.

It is important that the Privacy & Security Impact Assessment is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls.

The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation.

Privacy & Security Impact Assessments are an integral part of the "privacy by design" approach. This approach has been identified by the Information Commissioner and its approach is legally required under the GDPR.

Document Completion

A Privacy & Security Impact Assessment must be completed wherever there is a change to an existing process or service or if a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data or business critical information is handled.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (Stage 5). The project will need to be signed off by the implementer, a representative from Information Governance and a member of staff who has an appropriate level of responsibility for the project risks. Please note, sign off of this document does not close the privacy risks related to this project. It is important that the risks are revisited and any additional privacy risks identified are appropriately reviewed.

PLEASE NOTE:

The staff member (implementer) undertaking the Privacy & Security Impact Assessment has a responsibility to ensure that Patient Safety and Project initiation documentation are considered, in line with GOSH procedure.

PRIVACY & SECURITY IMPACT ASSESSMENT

Project Details

Project Title:	Trac.jobs role out
-----------------------	---------------------------

Project Description:

Describe in sufficient detail for the proposal to be understood. Explain broadly what project aims to achieve and what type of processing it involves. It may be useful to consider any benefits of the project.

You may find it helpful to refer or link to other documents, such as a project proposal.

Please see attached project plan

Staff involved in PIA assessment (Include Email Address):

Key Stakeholders:

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Additional Advice or considerations:

Please note that if this project is in anyway novel, uses state of technology or there are any current issues of public concern with regards to data collection and processing consulting information security experts or any other experts should be considered and any external guidance should be reviewed. Please document any consultation or materials considered.

Trac have provided the following PowerPoint.



Trac - Start Up
Summary - Jan 2019.

This gives a summary of the IG controls within the system and much of this information has been used to inform the rest of this document.



981543292383336-s
ervice-definition-docu

Service Definition outlines security in place for Trac's data storage. Information relating to hosting and security can be found within the service definition on our G Cloud entry:
<https://www.digitalmarketplace.service.gov.uk/g-cloud/services/981543292383336> (see service definition document on right hand side).

PRIVACY & SECURITY IMPACT ASSESSMENT

	 <p>Trac-Systems-G-Cloud-10_call-off_contract</p> <p>Trac Contract including processing agreement on page 35/36 (Schedule 7)</p>
--	---

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage 1 – Initial Screening Questions

Answering “Yes” to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full PIA will be undertaken on a case by case basis by Information Governance.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	
2	Will the project compel individuals to provide information about them?	Y	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure personal data is relevant, accurate and up-to-date?	Y	
6	Are there security arrangements in place while personal information is held?	Y	
7	Does the project involve using new technology to the organisation?	N	
If you have answered “Yes” to any of the questions numbered 1-7 please contact the Information Governance team to consider the requirement for further review.			

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage 2 – Privacy Impact & Security Assessment (Full)

Please answer the below questions in the boxes provided. To prevent duplication you may find it helpful to refer or link to other documents, such as project proposals or security documents.

If you have any queries with regards to any of the questions please contact the Information Governance Team.

2.1	What data will be collected?	
	Summarise the data that will be collected:	
	No patient information is processed. The system is used for data collection and storage of job applicants.	
	Personal Data: <i>Personal data is information that relates to an identified or identifiable individual.</i>	
	Identifiers (please specify) <i>This may include: name, identification number, location data; and an online identifier.</i>	The subject of the data collection <i>This may include: patients (please specify if this is a specific cohort of patients), families or relatives, staff; and members of the public.</i>
	All information collected through the application process	Employment applicants
	Staff names	Recruiting managers or HR admin roles
	Pseudonymised data (please specify) <i>Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.</i>	n/a
	Anonymised data (please specify) <i>Data is unlikely to be truly anonymous if users have access to other data which they could use to identify Data Subjects.</i>	n/a
	Special categories of personal data:	
	Racial or ethnic origin	<input checked="" type="checkbox"/>
	Political opinions	<input checked="" type="checkbox"/>

PRIVACY & SECURITY IMPACT ASSESSMENT

Religious or philosophical beliefs	<input checked="" type="checkbox"/>
Trade union membership	<input checked="" type="checkbox"/>
Genetic data	<input type="checkbox"/>
Biometric data	<input type="checkbox"/>
Health	<input checked="" type="checkbox"/>
Sex life	<input type="checkbox"/>
Sexual orientation	<input checked="" type="checkbox"/>
Data about criminal convictions or offences	<input checked="" type="checkbox"/>
Other data (please specify):	The above data may be collected as part of the application process

2.2	What format is the data? <i>Please specify if this data will be electronic or paper and the data types e.g. text, images, video etc.</i>
	All data will be collected electronically

2.3	If personal data is processed, what is the purpose? These maps to a Lawful basis for processing the data under Appendix A . This is mandatory for any processing of personal data.	
	Purpose	Example
	Direct care and Administrative Purposes	-Delivery of care -Sharing between individuals involved in care -Local clinical audit -Waiting list management - Performance against national targets
	Commissioning and planning purposes	-Legal requirements to provide data to health commissioners
	Research	-Studies with regards to patients with specific diagnosis
	Regulatory and public health functions	-Monitor health status to identify community health problems -Preparing for and responding to public health emergencies
	Safeguarding (following the provisions of the Children Acts 1989 and 2004,	-Safeguarding children and vulnerable adults

PRIVACY & SECURITY IMPACT ASSESSMENT

	and the Care Act 2014)	-Sharing information for a safeguarding purpose (i.e. with social work)	
	Employment	-Storing staff details -Contacting staff under employment laws	<input checked="" type="checkbox"/>
For any other purpose of processing personal data please contact the IG Manager to confirm the lawful basis for processing. This should be outlined below:			
	Purpose		
	Legal Basis for processing of personal data (Article 6, GDPR)		
	Legal Basis for processing of special categories of personal data (Article 9, GDPR)		

2.4	Is the data being collected necessary to perform the specified task?	
	Y/N	Please justify response Yes or No
	Y	All mandatory questions are required as part of the recruitment process.

2.5	Who are the Organisations or external individual involved in processing the data?	
	Organisations Name	Data Controller or Data Processor <i>The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.</i> <i>The Data Processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.</i>
	GOSH	Data Controller
	Trac	Data Processor

2.6	Will any information be held offsite or access given to any external parties?	
	Y/N	If Yes , an Information Sharing Protocol is required and outline document the controls. If data is stored in the Cloud please document the additional controls in place.
	Y	ISP provided to Trac to complete. The data will be hosted offsite.

PRIVACY & SECURITY IMPACT ASSESSMENT

		 <p>981543292383336-s ervice-definition-docu</p> <p>The above document has been provided and outlines the security requirements. This has been approved under G-Cloud 10. This has been provided in place of an ISP</p>
--	--	--

2.7	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered Yes
	Y	<p>The System will link with nhs jobs – to display new positions</p> <p>The System will also link with ESR to pull role info.</p>

2.8	Has the impact to other GOSH systems/processes been considered and appropriate leads consulted and in particular technical security?	
	Y/N	Please describe if answered Yes . Please state what checks were undertaken if response is answered No .
	Y	HR manages these system and with the help of trac are reviewing the new process.

2.9	How will the information be kept up to date and checked for accuracy and completeness? <i>e.g. demographic details will be checked against the SPINE, users be prompted to complete missing information</i>	
	All information is entered by data subjects themselves. The personal details are confirmed by the recruitment teams or recruiting managers as required.	

2.10	Who will have access to the information? (list individuals or staff groups)		
	Data	Staff Group/Individual Role	Justification for access
	Applicants	Recruitment teams	To assign managers for roles and general overview of the system and process at each point
	Applicants dependant on access	Recruitment users	access levels dependent on teams

PRIVACY & SECURITY IMPACT ASSESSMENT

	Applicants dependant on access	Managers	access granted on a vacancy by vacancy basis
--	--------------------------------	----------	--

2.11	<p>Is there an ability to audit access to the information? And is there a plan/process of how to run and monitor this? <i>i.e. are we able to review access, actions and use of accounts</i></p>		
	Y/N	Please describe if answered Yes . If NO what contingencies are in place to prevent misuse?	
	Y	<p>Auditing logging within system for users actions. e.g. <i>07-Nov-2014 14:09 sarah.halsey@abc.nhs.uk] Created</i> <i>[07-Nov-2014 14:09 sarah.halsey@abc.nhs.uk] Queued for posting to jobs.nhs.uk</i> <i>[07-Nov-2014 14:09 sarah.halsey@abc.nhs.uk] Review date set to 22-Nov-2014</i> <i>[07-Nov-2014 14:09 sarah.halsey@abc.nhs.uk] out to advert jobs.nhs.uk</i> <i>[07-Nov-2014 14:10 SYSTEM] Posted to jobs.nhs.uk, eligibility 1, closing date 21-Nov-2014</i> <i>[07-Nov-2014 14:32 SYSTEM] Result received from jobs.nhs.uk: Successful</i> <i>[24-Nov-2014 09:42 sarah.halsey@abc.nhs.uk] added shortlister</i> <i>[24-Nov-2014 09:42 sarah.halsey@abc.nhs.uk] Moved to Shortlisting; review date automatically updated to 27-Nov-2014</i> <i>[25-Nov-2014 10:00 brenda.whyt@abc.nhs.uk] Moved to Interview; review date automatically updated to 25-Nov-2014</i> <i>[26-Nov-2014 09:42 sarah.halsey@abc.nhs.uk] added interviewers</i> <i>[26-Nov-2014 09:45 sarah.halsey@abc.nhs.uk] Interviews set up; review date automatically updated to 11-Dec-2014</i></p> <p>Detailed audit logs are available upon request.</p>	

2.12	<p>How will access (or changes to access rights) be controlled? <i>Specify how changes in who should have access to the data will be administered</i> <i>e.g. linked to the Trust HR systems for leavers etc</i></p>		
------	--	--	--

PRIVACY & SECURITY IMPACT ASSESSMENT

	Recruitment team in HR will control access. General users will only have access to specific applications.
--	---

2.13	<p>What security measures have been implemented to control access? <i>e.g. Username and Password, link to Active Directory, Secure Token access, Key locked filing cabinet etc.</i></p>
	<ul style="list-style-type: none"> • Role-based user access via logons with strong password protection. • User access over encrypted HTTPS connection. • Firewalling. • Administration access restricted and secured. • Intrusion Detection System. • 24/7 monitoring. • Encrypted tunnels used for transit between systems. • Number of systems in use is minimised. All are owned and operated by Trac. • Anti virus. • Anti spam. • Server operating system patch regime; automated monitoring and alerting for patch availability. • Subscriptions to vulnerability alert databases.

2.14	What devices will be used to access the data and what controls have been implemented to secure these devices?	
	<p>Devices</p> <p><i>e.g. Trust computers, Any device with internet access</i></p>	<p>Security</p> <p><i>e.g. System access controls, device security requirements</i></p>
	Trust devices only	Secure to the level the Trust requires

PRIVACY & SECURITY IMPACT ASSESSMENT

2.15	Will data leave the Trust network? <i>i.e. can the data be accessed outside of the Trust</i>	
	Y/N	If Yes , outline any additional security elements.
	N	Data will be submitted by applicants but personal data will not generally be shared over the system.

2.16	Has staff training been proposed or undertaken and did this include confidentiality and security topic areas?	
	Y/N	Please describe if answered Yes
	Y	Training will be provided by trac to the relevant HR staff members. After this point userguides will be provided and new users/starters will trained by the team as required.

2.17	How will learning be supplemented and refreshed? <i>e.g. prompts at data entry, User guides, Standard Operating Procedures</i>	
	User guides will be provided by trac and can be adopted by GOSH. The recruitment team will be available to help with any questions managers have. The system has lots of help pages within it.	

2.18	Will reports be produced or can personal/sensitive personal or business confidential information be extracted? <i>i.e. can any users extract or export data from the new system</i>	
	Y/N	Please describe if answered Yes
	Y	Successful applicant packs can be downloaded and stored locally by the user organisation – i.e. stored in their HR file. Extracts will be able to be downloaded for shortlisting by managers etc
	Who will be able to run reports/extract?	Those with the ability to review
	What controls will be in place? <i>e.g. all extracts are automatically encrypted, exported data must be approved by admin</i>	These will be based on user education. This is true at the moment with NHS jobs.

PRIVACY & SECURITY IMPACT ASSESSMENT

2.19	Are plans in place for the retention and destruction of the data?	
	<i>These should be in line with the Records Management Code of Practice for Health and Social Care 2016</i>	
	Y/N	Please describe if answered Yes . Please state why not if response is No .
Y	Data is erased to schedule detailed in the Data retention and expiration policy. Successful applicant packs can be downloaded and stored locally by the user organisation and then retained as required.	

2.20	If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?	
	Y/N	Please describe if answered Yes . Please state why not if response is No .
	Y	All data can be exported and returned to GOSH – referenced in contract

2.21	Are disaster recovery and business contingency plans in place for the information? Additionally, are plan in place for how the system will be supported.	
	Y/N	Please describe if answered Yes . Please state why not if response is No .
	Y	Data centre has back up in place Locally GOSH will have business continuity plans in place.

2.22	Will individuals be informed about the proposed uses or sharing of their personal data?	
	Y/N	If Yes , please describe how. <i>e.g. updates to the Trust Privacy Notice, Information sheets provided or posters displayed etc.</i>
	Y	Trac will require user log ins and has its own privacy policy. https://apps.trac.jobs/
	If No , list the reason for not doing so <i>e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?</i>	

PRIVACY & SECURITY IMPACT ASSESSMENT

2.23	Are arrangements in place for recognising and responding to requests for access to data? <i>i.e. Requests for personal data under Data Protection Legislation or Requests for Corporate data under Freedom of Information Legislation</i>	
	Y/N	Please describe if answered Yes . Please state why not if response is No .
	Y	Requests for interview notes will be referred to HR who can extract specific records. Successful applicant data will be moved to the staff record and follow its rules for information releases.

2.24	Have you considered the rights of the Data Subjects and how you will comply with these?	
	The GDPR provides the following rights for individuals:	How will you comply with these rights
	The right to be informed (Question 2.22) <i>Individuals have the right to be informed about the collection and use of their personal data</i>	Privacy notice on the trac log in page and GOSH website
	The right of access (Question 2.23) <i>Individuals have the right to access their personal data</i>	GOSH SAR process
	The right to rectification <i>The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.</i>	Information is provided by applicants – can be adjusted if required.
	The right to erasure <i>The GDPR introduces a right for individuals to have personal data erased.</i>	Is required to be kept in line with legal requirements but each request would be considered. Trac accounts can be deleted.
	The right to restrict processing <i>Individuals have the right to request the restriction or suppression of their personal data.</i>	Applications can be withdrawn
	The right to data portability <i>The right to data portability allows individuals to obtain and reuse</i>	Data can be extracted straight from trac

PRIVACY & SECURITY IMPACT ASSESSMENT

	<i>their personal data for their own purposes across different services.</i>	
	The right to object <i>The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.</i>	These will be considered on a case by case basis.
	Rights in relation to automated decision making and profiling.	

2.25	Have Information Asset Owners (IAO) and Information Asset Administrators (IAA) been assigned?		
	<i>More guidance on these roles can be found on the Trust Intranet. It is suggested that one of these roles would belong to an individual who has been involved in the project.</i>		
	Roles	Name	Job Role
	IAO		
	IAA		

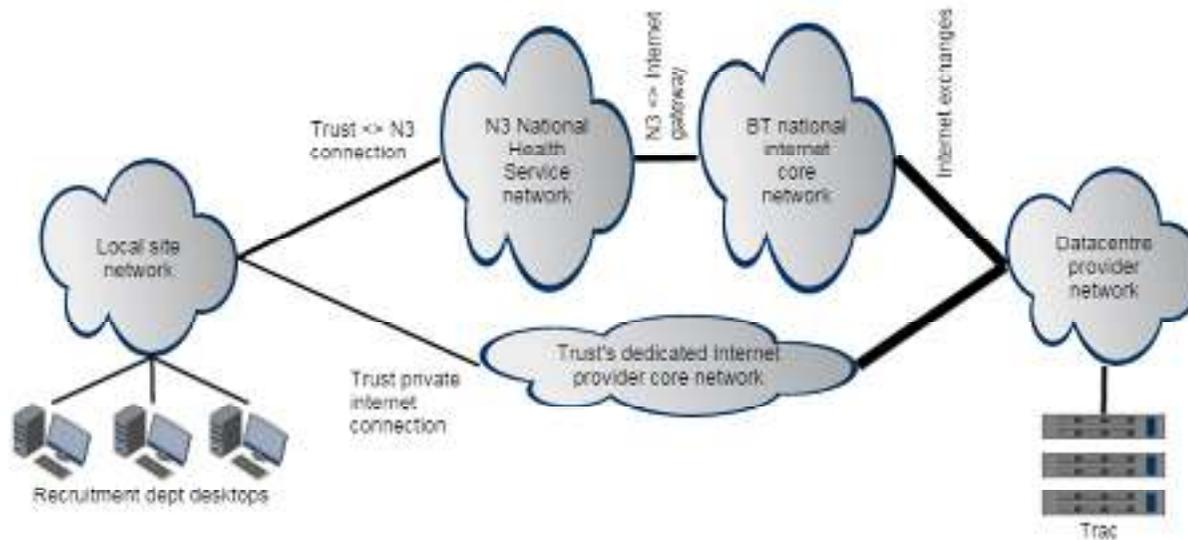
2.26	Has this been registered as an Information Asset Register ?	
	Y/N	If Yes , please provide the Information Asset Register reference number. If No , please state why.
	N	This will be added to the IAR

2.27	How will you prevent function creep? <i>i.e. how will you prevent or monitor the use of the technology or system beyond the purpose for which it was originally intended especially when this could leads to potential invasion of privacy</i>
	Functionality within the system is limited to recruitment.

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage - 3 Information Flow Mapping

Use this page to consider the transfers of information from one location to another. This is often most effectively mapped as a flow diagram which provides a visual interpretation of the flows of information and some of the controls referenced above. If a flow diagram is not used it may be suitable to describe the flows of information that will exist.



PRIVACY & SECURITY IMPACT ASSESSMENT

Stage - 4 Identified Risks and Mitigating Action

Use the provided table to document any privacy or information security risks identified from the above questions or additional risks that may exist. These could be to the Trust or data subjects. Examples may include inability to of individuals to exercise rights, illegitimate access or modification of personal data or loss of confidentiality. These risks should be scored using the Risk Assessment Matrix and for any risks considered 'High' or 'Medium' mitigating actions should be considered.

These may include:

- Deciding not to collect certain types of data
- Reducing the scope of the processing
- Taking additional technological security measures
- Training staff to ensure risks are anticipated and managed
- Anonymising or pseudonymising data where possible
- Writing internal guidance or processes to avoid risks
- Using a different technology
- Putting clear data sharing agreements into place
- Making changes to privacy notices
- Offering individuals the chance to opt out where appropriate
- Implementing new systems to help individuals to exercise their rights

When this table is completed it is important that any outstanding actions are assigned to an individual and documented. These actions could be incorporated back into an overall project plan.

Please note that any risks considered 'High' after mitigating actions have been applied should be alerted to the Information Governance Team as soon as identified.

A second table below the risks should be used to document any privacy benefits or improvements of the new system or process that is to be implemented. These may include added auditability, a requirement to collect less data than currently processed or additional security around information stored.

Knowledge of Impact	Adverse Effect	Low risk	High risk	High risk
	Some Impact	Low risk	Medium risk	High risk
	Minimal Impact	Low risk	Low risk	Low risk
		Positive	Reasonable possibility	More likely than not
Likelihood of Impact				

PRIVACY & SECURITY IMPACT ASSESSMENT

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary <i>If related to questions in stage 2 please reference the number</i>	Likelihood of harm Remote Possible Probable	Severity of harm Minimal Significant Severe	Overall risk Low Medium High	Options to reduce or eliminate risk Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk	Effect on risk Eliminated Reduced Accepted	Residual risk Low Medium High	Measure approved Yes/no	Mitigating Officer	Date to be completed:
Data extract – Staff will need to ensure any data extracted from Trac is processed and handled securely									
Hosted data – No ISP has been completed.				Information has been provided to the standard required for the Trust ISP for confirmation of security (2.6). This has been confirmed as part of the G-Cloud 10 contract.					
Vulnerability Test results have not been mitigated before go-live				These matters must be completed by the June 2019 release of the programme and written confirmation provided prior to the release.					

PRIVACY & SECURITY IMPACT ASSESSMENT

Please outline and potential privacy benefits or improvements from this implementation
These may include added auditability, a requirement to collect less data than currently processed or additional security around information stored.

--

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage 5 - Project Sign Off

	Name	Job Title	Organisation	Date
Project Lead				
Information Governance				
Responsible Owner (IAO)				
Data Protection Officer				

Assessment Summary

Summary of Privacy & Security Impact Assessment; including legislative compliance and identified risks:
Summary
Risks to GOSH
Risks to Data Subjects

Recommendations for Action

Summary of Identified Recommendations		
Recommendations	Recommendation Owner	Agreed Deadline for action

While this document can be signed off this does not close all risks. It should be reviewed if any additional privacy risks are identified at any stage in the life of the project and revisited if the use of personal data changes in any way. A copy should be kept by Information Governance and as part of the project documentation.

PRIVACY & SECURITY IMPACT ASSESSMENT

Appendix A

Legal Basis for using Personal Data

Purpose of using personal data	Examples	Conditions for lawful processing of personal data (Article 6 of GDPR)	Conditions for lawful processing special categories (including health) of personal data (Article 9 of GDPR)
Direct care and Administrative Purposes	<ul style="list-style-type: none"> -Delivery of care -Sharing between individuals involved in care -Local clinical audit -Waiting list management - Performance against national targets 	6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’	9(2) (h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’
Commissioning and planning purposes	-Legal requirements to provide data to health commissioners	6(1) (c) ‘...for compliance with a legal obligation...’ or 6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’	9(2) (h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’
Research (GOSH will still require consent or an appropriate legal basis (e.g. section 251 support) that meets confidentiality and ethical requirements to use personal identifiable data for research)	-Studies with regards to patients with specific diagnosis	6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’	9(2)(j) ‘...scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate...and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject ...’
Regulatory and public health functions	<ul style="list-style-type: none"> -Monitor health status to identify community health problems -Preparing for and responding to public 	6(1) (c) ‘...necessary for compliance with a legal obligation...’	9(2)(l) ‘...necessary for reasons of public interest in the area of public health...or ensuring high standards of quality

PRIVACY & SECURITY IMPACT ASSESSMENT

	health emergencies		and safety of health care and of medicinal products or medical devices...'
Safeguarding (following the provisions of the Children Acts 1989 and 2004, and the Care Act 2014)	-Safeguarding children and vulnerable adults -Sharing information for a safeguarding purpose (i.e. with social work)	6(1) (e) '...for the performance of a task carried out in the public interest or in the exercise of official authority...'	9(2)(b) '...is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of ...social protection law in so far as it is authorised by Union or Member State law..'
Employment	-Storing staff details -Contacting staff under employment laws	6(1) (e) '...for the performance of a task carried out in the public interest or in the exercise of official authority...'	9(2)(b) '...is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment...social protection law in so far as it is authorised by Union or Member State law..'