Great Ormond Street Hospital for Children NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Child Protection Information Sharing – Social work process and Spine integration	

Version History:

Date	**Version**	**Author name and designation**	**Summary of main changes**
April 2019	Draft	Joseff Eynon-Freeman, Information Governance Manager	DPIA replaces the previous Privacy Impact Assessment.

DATA PROTECTION IMPACT ASSESSMENT

Introduction

A Data Protection 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 Data Protection 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 Data Protection 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.

Data Protection 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 Data Protection 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 signed by a minimum of 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.

Further guidance for completing a DPIA can be found on the Process for completing Data Protection Impact Assessment Documents on the Intranet or by contacting the IG Team on Your.Data@gosh.nhs.uk.

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.

DATA PROTECTION IMPACT ASSESSMENT

Project Details

Project Title:	**Process for use of Child Protection Information Sharing**

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.

https://digital.nhs.uk/services/child-protection-information-sharing-project

Previous PIA completed 2016 included in the below initial project brief.

Privacy Impact
Assesment - CP-IS v1

Process is changing from a manual check to an automated process so this DPIA has been updated to reflect this.

Staff involved in PIA assessment (Include Email Address):	Safeguarding IG Manager

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.*	

Intended Go-Live date for the project	

DATA PROTECTION 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 assessment will be undertaken on a case by case basis by Information Governance.

Update on previous DPIA as process has changed. See project description above

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

DATA PROTECTION 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:

The below is a summary of the process and where information is collected/shared.

1. Patient is added to Epic
2. If certain criteria are met, the patient's demographic details are queried against the NHS Spine, unless they already have a CP FYI flag or have been queried against the Spine in the last 30 days with a match.
    a. These triggers are if the patient attends, DNAs, is admitted, has home leave or is discharged.
3. If the patient has a Child Protection Plan recorded on the Spine a match email is sent to a generic CPIS social work email with restricted access
4. The email includes the patient demographic details, the Local Authority that issued the plan, other organisations that have triggered an alert i.e. viewed the record on the Spine and the type of plan
5. The content of the email is then copied to the patient record as an FYI flag on Epic and a Social Work order is created for the Social Work Team to review the patient/follow up with the Local Authority
6. The email is then moved to the appropriate inbox folder and then deleted after one month (evidence of all Spine queries are saved in a secure database)

Personal Data:

Personal data is information that relates to an identified or identifiable individual.

Identifiers (please specify) *This may include: name, identification number, location data; and an online identifier.*	The subject of the data collection *This may include: patients (please specify if this is a specific cohort of patients), families or relatives, staff; and members of the public.*
On entry to Epic patient records would be queried automatically against the Spine and an alert emailed to CPIS inbox if a Plan is in place. Details within the plan are not in scope (these may be requested by Social Work from the Local Authority if appropriate as part of the created order)	Patient

	Pseudonymised data (please specify) *Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.*	
	Anonymised data (please specify) *Data is unlikely to be truly anonymous if users have access to other data which they could use to identify Data Subjects.*	
	Special categories of personal data:	
	Racial or ethnic origin	☐
	Political opinions	☐
	Religious or philosophical beliefs	☐
	Trade union membership	☐
	Genetic data	☐
	Biometric data	☐
	Health	☒
	Sex life	☐
	Sexual orientation	☐
	Data about criminal convictions or offences	☐
	Other data (please specify):	

2.2	What format is the data? *Please specify if this data will be electronic or paper and the data types* *e.g. text, images, video etc.*
	Automated electronic check, then email

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, and the Care Act 2014)	-Safeguarding children and vulnerable adults -Sharing information for a safeguarding purpose (i.e. with social work)	☒
	Employment	-Storing staff details -Contacting staff under employment laws	☐
	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	The data collected is the only that a Protection Plan is in place, this should be already know to the team on referral and can have a direct impact on the care delivery to a patient. No details of the plan are shared over this process and these will continue to be accessed over the current methods of contact with Local Authorities.

2.5	Who are the Organisations or external individual involved in processing the data?

	Organisations Name	Data Controller or Data Processor *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.* *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.*
	GOSH	Data Controller for patient demographics (initial query)
	NHS Digital	Data Controller (any data pulled from the Spine)
	Patients Local Authority	Data Controller (any CP plan for a patient)

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	Information will be pulled from the Spine through the automated process. If a plan in requested by GOSH from the LA as a result this is out of scope but would be done securely (usually via nhs.net) on an ad hoc basis.

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	A new process has been designed to query the Spine with patient demographics.

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	ICT have been fully involved and built new process to query the Spine.

2.9	How will the information be kept up to date and checked for accuracy and completeness? *e.g. demographic details will be checked against the SPINE, users be prompted to complete missing information*
	The data is not acted on directly to impact care. When an alert is generated and an order put in to Social Work a decision is made how to act on it. i.e. they may already be aware of

	the request or may contact the LA for more information.

2.10	Who will have access to the information? (list individuals or staff groups)		
	Data	Staff Group/Individual Role	Justification for access
	Email alert from Spine check	CSPs and Safeguarding have access to the CPIS inbox	To input the data onto Epic
	Data inputted on Epic	All staff with Epic access	Details required for patient care
	Database which stores evidence of look ups, failed look ups, patients without LA,	2 Safeguarding and ICT Admin	To audit and query results

2.11	Is there an ability to audit access to the information? And is there a plan/process of how to run and monitor this? *i.e. are we able to review access, actions and use of accounts*	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	No audit functionality within email. Epic has full auditability. The database will store an audit of all queries run.

2.12	How will access (or changes to access rights) be controlled? *Specify how changes in who should have access to the data will be administered* *e.g. linked to the Trust HR systems for leavers etc*
	Safeguarding team will control access to the Database and CPIS email inbox

2.13	What security measures have been implemented to control access? *e.g. Username and Password, link to Active Directory, Secure Token access, Key locked filing cabinet etc.*
	Email and Database access based on Active Directory Epic Access controlled by Epic

2.14	What devices will be used to access the data and what controls have been implemented to secure these devices?	
	Devices *e.g. Trust computers, Any device with internet access*	Security *e.g. System access controls, device security requirements*
	Data will only be stored on current Trust systems which have access controlled.	

2.15	Will data leave the Trust network? *i.e. can the data be accessed outside of the Trust*	
	Y/N	If **Yes**, outline any additional security elements.
	Y	A secure connection to the NHS Spine has been set up to query patient details.

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	Specific training has been given to CSPs if required to check out of hours.

2.17	How will learning be supplemented and refreshed? *e.g. prompts at data entry, User guides, Standard Operating Procedures*
	A SOP will be created to remind staff of all the steps in the process.

2.18	Will reports be produced or can personal/sensitive personal or business confidential information be extracted? *i.e. can any users extract or export data from the new system*	
	Y/N	Please describe if answered **Yes**
	Y	Reports may be created from the Database. The access will be very limited to how these are used.

	Who will be able to run reports/extract?	
	What controls will be in place? *e.g. all extracts are automatically encrypted, exported data must be approved by admin*	

2.19	Are plans in place for the retention and destruction of the data? *These should be in line with the Records Management Code of Practice for Health and Social Care 2016*	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	This will form part of the patient record and information will be retained in line with Trust process.

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	Data will be stored as part of the main patient record.

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.**
	N	Specific plans not in place but if the process is disrupted Safeguarding staff still have access to query the Spine directly using their Smartcard access.

2.22	Will individuals be informed about the proposed uses or sharing of their personal data?	
	Y/N	If **Yes**, please describe how. *e.g. updates to the Trust Privacy Notice, Information sheets provided or posters displayed etc.*
	Y	Trust Privacy Notice specifically mentions sharing of social work information with other parties.
	If **No**, list the reason for not doing so *e.g. relying on an existing agreement, consent is implied, the project has s251 approval or*	

	other legal basis?

2.23	Are arrangements in place for recognising and responding to requests for access to data? *i.e. Requests for personal data under Data Protection Legislation or Requests for Corporate data under Freedom of Information Legislation*	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	This will form part of the patient's medical record. As this is safeguarding information it will be reviewed by a safeguarding professional before release in line with process.

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) *Individuals have the right to be informed about the collection and use of their personal data*	See 2.22
	The right of access (Question 2.23) *Individuals have the right to access their personal data*	See 2.23
	The right to rectification *The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.*	The Data Controller would be the Local Authority and if there were challenges to the CP this would need to be raised with them.
	The right to erasure *The GDPR introduces a right for individuals to have personal data erased.*	The Data Controller would be the Local Authority and if there were challenges to the CP this would need to be raised with them.
	The right to restrict processing *Individuals have the right to request the restriction or*	The Data Controller would be the Local Authority and if there were challenges to the CP this would need to be raised with them.

	suppression of their personal data.	
	The right to data portability *The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.*	See 2.23
	The right to object *The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.*	The Data Controller would be the Local Authority and if there were challenges to the CP this would need to be raised with them.
	Rights in relation to automated decision making and profiling.	While the pull of data from the Spine is automated no decision around patient care will be made within human decision making.

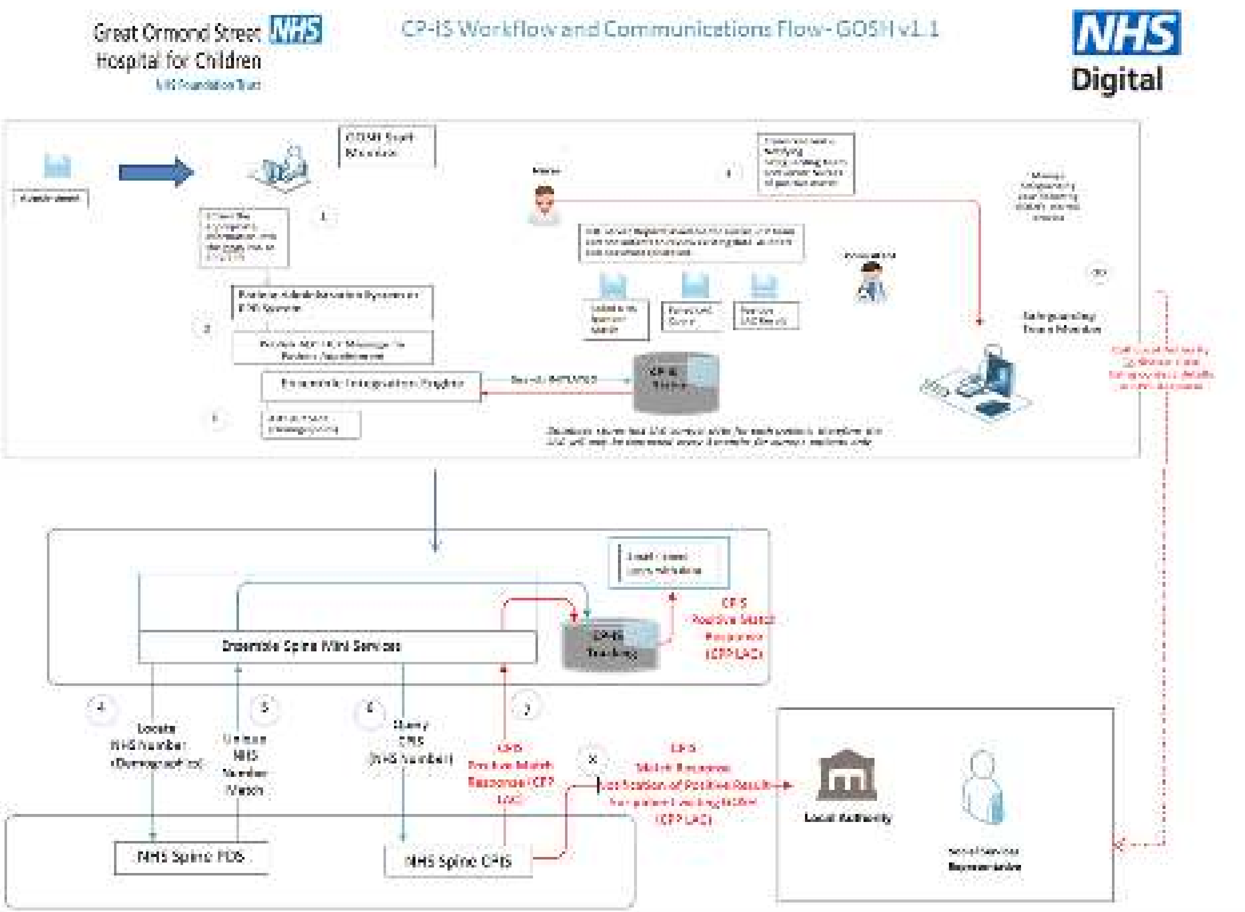
2.25	Have Information Asset Owners (IAO) and Information Asset Administrators (IAA) been assigned? *More guidance on these roles can be found on the Trust Intranet. It is suggested that one of these roles would belong to an individual who has been involved in the project.*			
	Roles	Name	Job Role	Email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

2.27	How will you prevent function creep? *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*
	This process is very restricted in function. If this was to be expanded to search for more data on the Spine this would require a review of the process.

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.


Great Ormond Street Hospital for Children
NHS Foundation Trust
CP-IS Workflow and Communications Flow - GOSH v1.1
NHS Digital
GOSH Staff Member
1
2
3
4
5
6
7
Patient Administration System or EPR System
Electronic Integration Engine
CP-IS Status
Safeguarding Team Member
Ensemble Spine Mini Services
CPIS Tracking
CP-IS Positive Match Response (CP? LAC)
Locate NHS Number (Demographics)
Unique NHS Number Match
Query CPIS (NHS Number)
CPIS Positive Match Response (CP? LAC)
CPIS Match Response Notification of Positive Result for patient (CP? LAC)
Local Authority
Social Services Representative
NHS Spine PDS
NHS Spine CPIS

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.

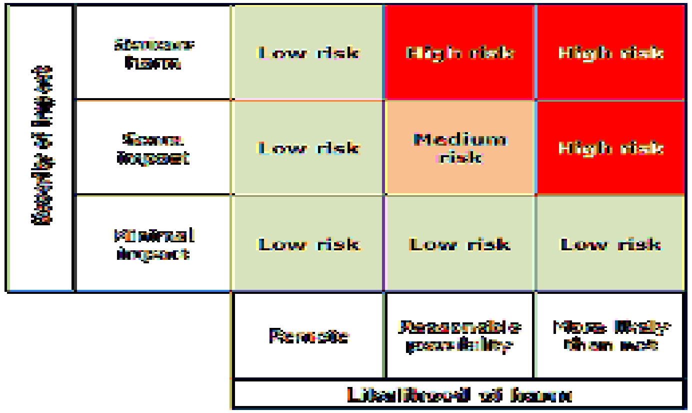
These may include:

- 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.



Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

PRIVACY & SECURITY IMPACT ASSESSMENT

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary *If related to questions in stage 2 please reference the number*	**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:**
Consent- Public perception of information shared without their knowledge or consent. This may cause lack of Trust to the Hospital. GOSH is also the first organisation to expand the check for unscheduled admittance only.	Remote	Minimal	Low	The Trust does identify that information will be shared with other social work providers on its privacy notice but does accept this may not be viewed by all families. Families are fully informed in when a Protection plan is put in place that this should and will be accessible to all care providers. This risk has been identified by overarching project for NHS Digital.	Accept				

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.

Stage 5 - Project Sign Off

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

Assessment Summary

Summary of DPIA; including legislative compliance and identified risks:
Summary
Risks to GOSH
Risks to Data Subjects

Recommendations for Action

Summary of Identified Recommendations

If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

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.

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	-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	-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)(I) ' …necessary for reasons of public interest in the area of public health…or ensuring high standards of quality

	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..’