Great Ormond Street Hospital for Children NHS Foundation Trust

Privacy & Security Impact Assessment

Title	Ref number
Order and view	

DRAFT

PAGE							
ISSUE	1						
DATE	07/04/2019						

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 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:	*NGS panel data 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.

This project involves a link from GOSH to Royal Marsden Hospital for submitting of genetic tests using the Order and View system. Demographic data will be submitted on the system, the sample shared with the generated order number, and then the test results provided back to GOSH on the system. These results are then extracted and saved to the GOSH patient record.

Order and View Information Pack

O&V Information Pack Final v1.1.doc

Terms and Conditions

O&V Terms and Conditions V3.0.doc

Staff involved in PIA assessment (Include Email Address):	[redacted]

Key Stakeholders: *Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.*	[redacted]

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*	At the time of writing (07/04/2019) this is to allow staff at GOSH to order and view reports with Royal Marsden using a web based application hosted by RMH.

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.	

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	Demographic data to enable unequivocal identification of patient
2	Will the project compel individuals to provide information about them?	N	
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	Personal data is checked and verified at the point of collection.
6	Are there security arrangements in place while personal information is held?	Y	Even though this data uniquely identifies an individual the data is only available to staff with a login.
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:	
	Patient demographic data, name DOB and lab ID will be collected to order a test. Sequence data will be collected and viewed. Sample will be shared with RMH and results returned to GOSH on the system.	
	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.*
	GOSH Lab ID	Sample ID within GOSH system
	RMH lab ID	Sample ID within RMH system
	DOB	Patient
	Name	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.*	The sample ID which can link back via GOSH systems to the GOSH patient.
	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.*	None
	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.*
	Electronic (physical sample will be shared by secure courier)

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	Demographic data to identify genetic data for the purpose of delivery of care to the patient

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.*
	Royal Marsden Hospital	Generates genetic data from sample (Data Processor)
	GOSH	Data Controller

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	Data will be held off GOSH site within Royal Marsden. The below ISP is to be signed by GOSH and RMH

		 Data Access and Information Sharing 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**
	N	Data will be extracted as a pdf from the system and saved in line with the current process. It has been confirmed that a note and the relevant clinical detail will be added in the record on Epic (within beaker) and a SOP is in place for to ensure that each result will be extracted and stored on a secure drive. The storage of the pdfs will be considered if this can be added to On Base.

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.**
	N	No other departments involved

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*
	This is an automated system and the information will be checked at the time of collection and input.

2.10	Who will have access to the information? (list individuals or staff groups)		
	Data	Staff Group/Individual Role	Justification for access
	Demographics	SIHMDS-AG / RMH	Identification of patient
	Genetic data	SIHMDS-AG / RMH	Data required for healthcare

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?
	N	Only staff necessary to provide service will be given logins. This will be managed by a local admin in the Trust.

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*
	Access will be granted by system administrator. Lead Healthcare Scientist will be the Trust admin.

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.*
	Username and password

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*
	Trust computers	Trust logins will be required as this will go over the N3 network – therefore accessible only through the Trust network.

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	Direct encrypted link to RMH and encrypted links to cloud storage. Data at rest will also be encrypted

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	Trust IG refreshed annually and mandatory. Ethical training refreshed annually and recorded by departmental training officer. SOPs and user guides are provided by RMH and a local SOP is in development.

2.17	How will learning be supplemented and refreshed? *e.g. prompts at data entry, User guides, Standard Operating Procedures*	
	Mandatory annual reassessment. SOP and user guides will be available – supplied by RMH	

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	Results from the processing of the supplied genetic data will be issued to clinician. Once the PDF is extracted it will be interpreted and the information will be stored into Beaker (Epic Module). The PDF will then be stored in the same location, it always has been stored which is the I Drive. This will be reflected in the SOP	
	Who will be able to run reports/extract?		Processor of the genetic sample
	What controls will be in place? *e.g. all extracts are automatically encrypted, exported data must be approved by admin*		Trust login Encryption Training

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	All data is stored for minimum of 30 years within GOSH but to be reviewed in line with retention periods and process before destruction. It will be removed from the RMH system at set intervals.

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 would be destroyed as directed by Trust policy. All data will be extracted by the team to Trust records when available.

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.**
		Please refer to the ISP at 2.6

2.22	Will individuals be informed about the proposed uses and share 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.*
	N	
	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?*	
	Consent is implied. This will be developed further as part of the projects with the GLHs but steps will be taken to inform patients that when they receive genetic testing this test will take place in a 'virtual lab' . The next update to the Trust Privacy Notice will include explicit reference to this sharing while it is only a general update of sharing within NHS for continuing care at the moment.	

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*

PRIVACY & SECURITY IMPACT ASSESSMENT

	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Dealt with by current Trust process and will be reflected in the SOP. i.e. When a request comes in for a record this will be processed by the Health Records Team. They will then review the medical record and produce a release of information. If genetic information existed outside of the record this would be documented in beaker with the clinical interpretation.

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*	2.22
	The right of access (Question 2.23) *Individuals have the right to access their personal data*	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.*	Patients would but unable to rectify genetic test results. If demographic details were to be requested changed this would need to be a manual process for completed pdf results i.e. amendments added
	The right to erasure *The GDPR introduces a right for individuals to have personal data erased.*	Any request to erase clinical data would need to carefully consider. This would require clinical consideration (likely from the Trust Caldicott Guardian) whether it is appropriate to grant the request or not. I.e. does the individual understand the risks and aware of the implications. In some cases requests for erasure may be denied.
	The right to restrict processing *Individuals have the right to request the restriction or suppression of their personal data.*	The same process as the right to erasure above would be followed.
	The right to data portability *The right to data portability allows individuals to obtain and reuse their personal data for their own*	The Trust would release this information however it is stored. This is only in pdf at this time.

	purposes across different services.	
	The right to object *The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.*	The same process would be followed as the right to erasure.
	Rights in relation to automated decision making and profiling.	Automated decision making is not part of this process however if this changes this document will be updated.

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	Tbd	Lead for genetics	
	IAA	[redacted]	Lead Healthcare Scientist	

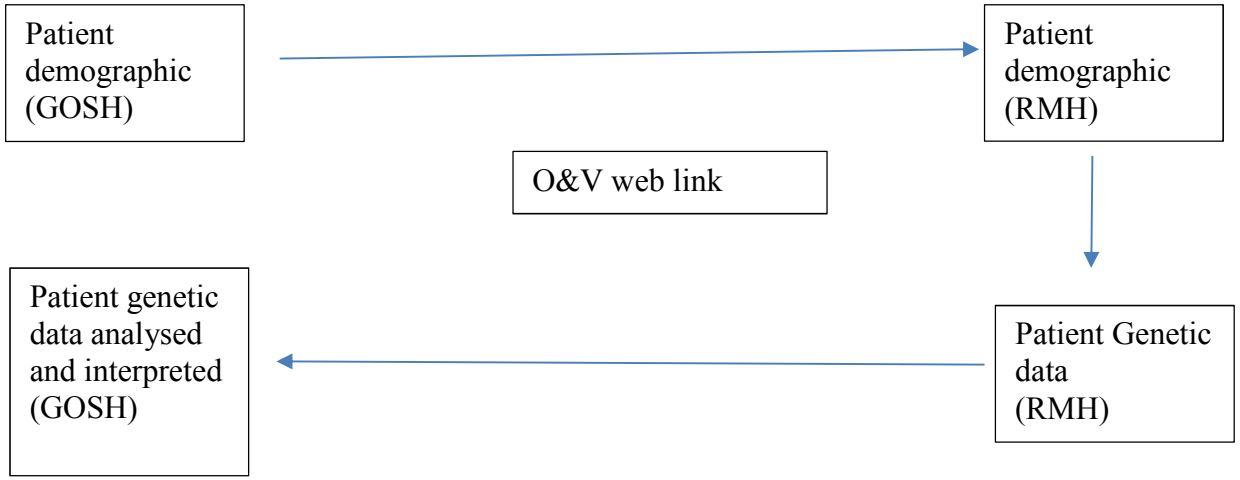
2.26	Has this been registered as an Information Asset Register?	
	Y/N	If **Yes**, please provide the Information Asset Register reference number**.** If **No**, please state why.
		This will be registered on the IAR

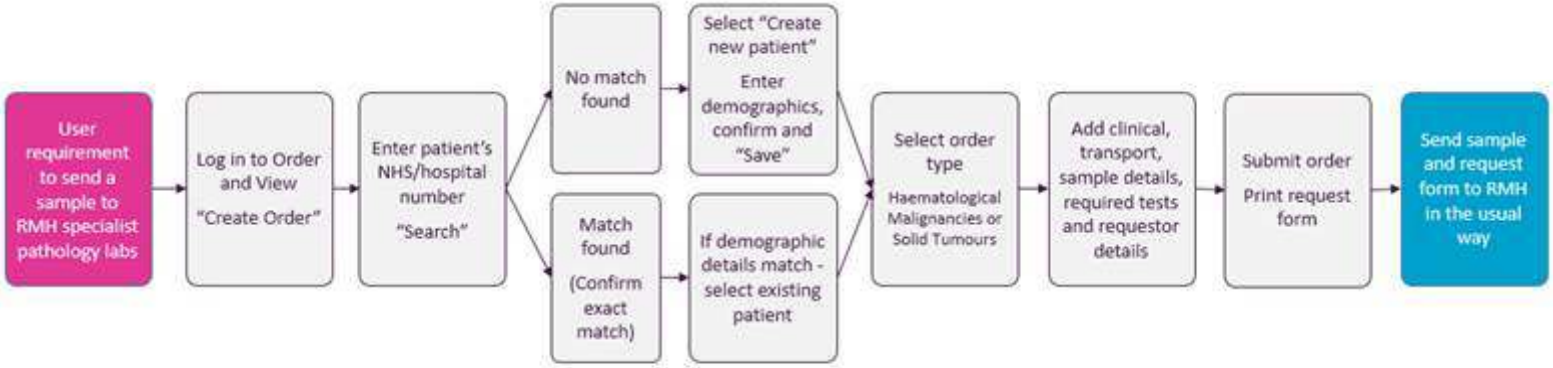
2.27	How will you prevent function creep? *i.e. how will you prevent or monitor the use of the technology or system beyond the purpose for which it was originally intended especially when this could leads to potential invasion of privacy*
	The system has limited functionality and will only be used to capture the demographics for testing and the results will then be exported to the patients record. This will be reinforced through training

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. Helena





Description:

This workflow explains the process for creating a pathology order and sending a sample to RMH	Log in to the online Order & View system using your secure user ID and password and select 'Create Order'	Search for an existing patient using NHS/hospital number or demographic information	If your search returns a match, check that all demographic details match, select the patient and proceed If the patient does not exist in the system, create a new record by entering patient details and demographic information, tick the checkbox to confirm details are correct and proceed	Select which type of pathology investigations you require	Add information such as clinical requirements, transport and requestor details	Submit your order and **print the request form**, this must be physically attached to the sample	Send the sample and request form to RMH in the usual way

Stage - 4 Identified Risks and Mitigating Action

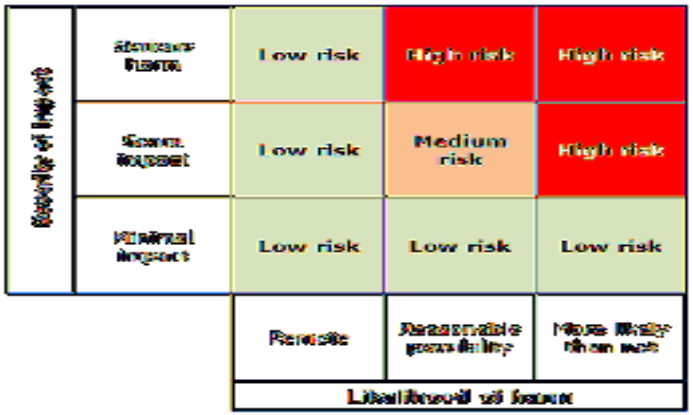
Use the provided table to document any privacy or information security risks identified from the above questions or additional risks that may exist. These could be to the Trust or data subjects. Examples may include inability to of individuals to exercise rights, illegitimate access or modification of 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.

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:**
Data processed by an external provider. (2.6)	Possible	Significant	Medium	-Complete the ISP – signed by both parties - this confirms the arrangements in place by RMH are deemed appropriate by GOSH	Reduced	Low	Yes	[redacted]	**11/09/2019**
Patient data being processed by an external party	Remote	Minimal	Low	Steps will be taken to inform patients their data will be processed by another provider but this is seen as low risk. The testing will be undertaking fully within the NHS for direct patient care and access to patient identifiable data is highly controlled and auditable. When genetic testing is realigned national there will be a large communication plan around this.	Accepted				

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.
This is the first step in improving efficiencies for genetic testing nationally were different NHS labs specialising in different tests can submit and share orders securely. The data will be transferred securely. All transfers will be secure and automated to replace any existing links which would have relied on user emails.

Stage 5 - Project Sign Off

	Name	Job Title	Organisation	Date
Project Lead	[redacted]		GOSH	
Information Governance			GOSH	01/08/19
Responsible Owner (IAO)				
Data Protection Officer				

Assessment Summary

Summary of Privacy & Security Impact Assessment; including legislative compliance and identified risks:
Summary
The risks are minimal and this should be seen as improving the securely and transfer of patient data between two sites. GOSH data will continue to be processed by RMH but in a more structured way. An ISP will be in place to ensure the storage and processing of the data is done so in an appropriate way.

Recommendations for Action

Summary of Identified Recommendations		
Recommendations	**Recommendation Owner**	**Agreed Deadline for action**
Add the system to IAO	[redacted]	**As soon as patient data is to be added**
Create SOP and procedure documents- there is an understanding that these documents will need to be developed to fit local procedure but the RMH standard templates can be utilised until GOSH develops its own.		**TBD**
ISP to be signed		**Before go live**

PRIVACY & SECURITY IMPACT ASSESSMENT

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..'