Greater Manchester Shared Services

Privacy Impact Assessment (PIA) Proforma

Reference: 00
PIA Title: Transporting of electronic images
Version: 1.0
Date: 13 November 2018

DOCUMENT CONTROL PAGE	
Title	Privacy Impact Assessment Proforma
Version	3.0
Date	December 2017
Review	December 2019

Why do I need to complete a Privacy Impact Assessment?

Data protection impact assessments (DPIAs) help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

A PIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

Please note the template is constantly being changed / updated to meet new requirements so always make sure you use the latest version.

When do I complete a Privacy Impact Assessment?

If you are doing any of the following:

- setting up a new process whether you are using personal confidential data (PCD) or not a PIA should be completed and filed with the project paperwork
- changing an existing process which changes the way personal confidential data is used
- procuring a new information system which holds personal confidential data

They must be completed as early as possible to ensure risks can be identified and mitigated to an acceptable level.

Who needs to complete a Privacy Impact Assessment?

It is the Information Asset Owners responsibility to ensure this is completed and submitted. They can delegate this task to an Information Asset Administrator (IAA) / Project Manager and or suppliers of a system / asset.

PIA Process Flowchart

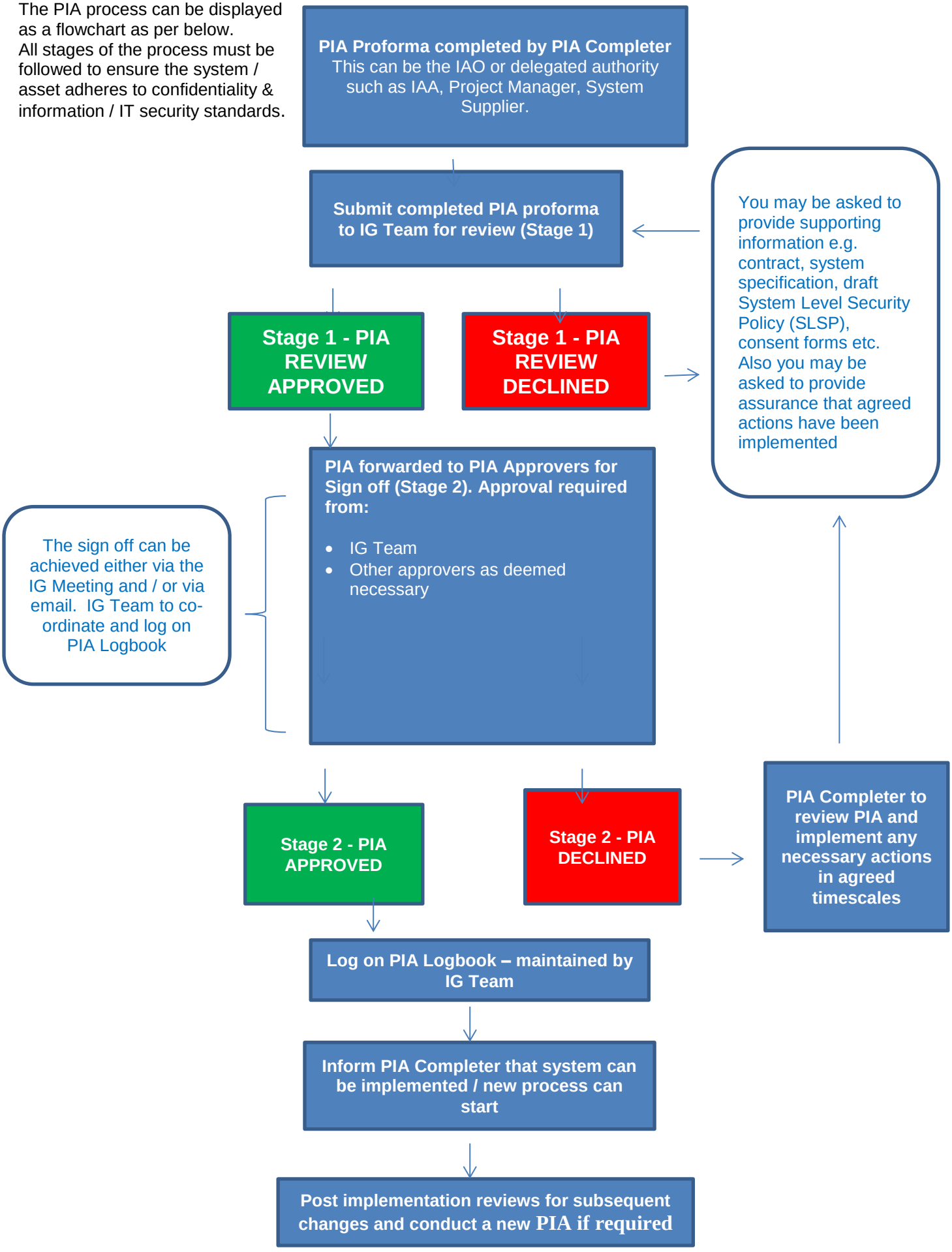
Please complete each section (where applicable) with as much information as possible. For example, a key piece of information is who the Information Asset Owner and Information Asset Administrator will be for a system / asset.

The following flowchart highlights the steps once the PIA has been completed until either approval and / or rejection decision has been reached.

Privacy Impact Assessment Process Flowchart

Greater Manchester Shared Services

The PIA process can be displayed as a flowchart as per below.
All stages of the process must be followed to ensure the system / asset adheres to confidentiality & information / IT security standards.



Important

By completing this Privacy Impact Assessment, all parties associated with the PIA agree to adhere to the IG Toolkit requirements and have Information Governance and Information Security Policies in place as follows:

- System Level Security Policy including Business Continuity Plan
- Data Protection Procedure
- Information Governance Policy
- Completion of Information Governance mandatory training
- Information Governance Incident Reporting Procedures
- Safe Transfers of Information Procedure
- Information Asset Register

The list above is not exhaustive.

In the event of an incident and failure to have the above may incur to a larger monetary penalty being levied upon you by the Information Commissioners Office (ICO).

Screen 1: PIA Completed by:

Organisation	Name	Date	Signature
Click here to enter text.	Click here to enter text.	Click here to enter a date.	

For completion by: IG/Approval Group

Approved – no actions required	☒	**21/11/2018**
Approved with action plan	☐	Click here to enter a date.
Declined (give reason)	☐	Click here to enter text. Click here to enter a date.

Screen 2: Basic Information

PIA Completer Name: *(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	
Department:	Effective Use of Resources Team
Email:	
Telephone No.:	
Process Name:	Transportation of electronic images
New System Supplier Name: **(if applicable):**	N/A – this is a change to an existing process
Date System due to go live (if applicable):	22 November 2018
Project Proposal / Purpose for completing PIA:	As part of the decision making process the EUR Service currently receives electronic images (photographs and occasionally videos) from clinicians, patients and carers which are annoymised and shared with Individual Funding Panels so that they can review the images alongside written evidence when making a decision about a patient's treatment. These images have in the past been shared with the panels in paper format. This PIA has been completed to request a change to the process of transporting images. Rather than taking hard copies of the images to an IFR Panel meeting, for consideration, the GMSS EUR Service is seeking authorisation to 1) load them on to a work laptop which will then be shared with panel members in the meeting and 2) email them to a secure CCG email, password protected for panel members to view. Following the meeting the images will then be deleted from the laptop if option 1 is chosen by the EUR Service. The laptops are work devices and therefore are encrypted and can only be accessed via a Bitlocker PIN followed by the users own log-in details. Both options present a more secure way of transporting the material. The EUR Service is seeking approval for both options, however it is envisaged that only one option per panel meeting will be used at any one time. However having both options authorised will allow the EUR service greater flexibility and resilience when deciding how to transport electronic images

Link to any wider initiative: *(if applicable)*	N/A but would support the initiative to move to going paperless
Information Technology involvement	List any applicable electronic systems/software to this initiative (current and/or new):

System name	**Used by e.g. organisation and dept.**	**Parties/system supplier**
Current laptops	GMSS	GMSS
Current nhs.net secure email address	GMSS	NHS Digital

Are any other organisations are involved in this initiative?	The 10 GM CCG's already receive images in hard copy tables at the meeting. This new process will remove the need to take hard copies to the meetings. Instead the EUR member of staff will either email the images ahead of the meeting or load them on to a laptop for viewing within the meeting. All 10 Greater Manchester CCG's would be affected by this change. The images would be transported and viewed using the team's laptops or viewed via secure CCG email address.

Confirm all relevant organisations have or are working towards cyber essentials

Organisation/Parties/ system supplier	**Cyber essentials Y/N Working towards/cyber compliance defined under terms of contract**
N/A GMSS doesn't currently have cyber essentials	

Is this initiative in line with or achieving national or local guidance/ strategy or mandate?	This initiative is in line with going paperless and offers a more secure way of transporting and sharing photographic evidence.

Screen 3: Screening Question

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☒	☐	☐	The images are of areas of a patient's body and are used as part of a decision making process. Therefore they need transporting securely. Currently a hard copy is taken by the EUR Service and tabled on the day.
b)	Will the initiative involve the collection of new information about individuals?	☐	☒	☐	Images are already collected as part of the decision making process and shared with a panel. This PIA is around changing the way images are transported
c)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☒	☐	Images are already collected as part of the decision making process and shared with a panel. This PIA is around changing the way images are transported
d)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☐	☒	☐	We already receive this information. See above.
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☒	☐	IFR Panels have previously had access to the images – however this has been in paper form in the past tabled at the meeting.
f)	Does the initiative involve you using new technology which might be perceived as being	☐	☒	☐	Rather than taking hard copies to the meeting they will be shared electronically

	intrusive? e.g. biometrics or facial recognition				by being stored on a work laptop or sent to a secure email and password protected.
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☒	☐	☐	IFR Panels will make a decision based on the images and written information. This already happens when they receive the images in paper format – so the decision making would remain unchanged.
h)	Will the initiative compel individuals to provide information about themselves?	☐	☒	☐	Patients and clinicians already provide the service with electronic images which are shared with an IFR Panel in paper format. Patients and clinicians are not mandated to send images in, but if they feel that the request is strengthened by images then they can be submitted. Otherwise a decision will be made on the basis of the information held.

If you answered **YES or UNSURE** to any of the above you need to continue with the Privacy Impact Assessment.

***Sign off if no requirement to continue with Privacy Impact Assessment*:**	
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Privacy Impact Assessment	
Agreed by:	Click here to enter name of group or individual(s).

Screen 4: Contact Information

Project Manager:	
Project Manager Email:	
Project Manager Telephone No.:	
Information Asset Owner (IAO) Details	
IAO Name:	
IAO Title:	
IAO Department:	
IAO Email:	
IAO Telephone Number:	
Information Asset Administrator (IAA) Details	
IAA Name:	
IAA Title:	
IAA Department:	
IAA Email:	
IAA Telephone Number:	

Screen 5: Personal Confidential Data Items

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Personal details	Information that identifies the individual and their personal characteristics	Check all that apply: ☐ Forename(s) ☐ Surname ☐ Address ☐ Postcode ☐ Date of Birth ☐ Age ☐ Gender ☐ Physical description ☐ Home Telephone Number ☐ Mobile Telephone Number ☐ Other Contact Number ☐ Email address ☐ GP Name and Address ☐ Legal Representative Name (Next of Kin) ☐ NHS Number ☐ National Insurance Number ☑ Photographs/Pictures of persons ☐ Other – if this is ticked please list 'Other' personal data items to be processed below: See attached	Photograph or video evidence of a patient's condition to support the decision making process is shared with a CCG IFR panel. This PIA is to request a change in process so that images are shared more securely.
Physical or mental health or condition	Information relating to the individuals physical or mental health or condition. NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the	☑ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Photograph or video evidence of a patient's condition to support the decision making process is shared with a CCG IFR panel. This PIA is to request a

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
	Mental Health Act.		change in process so that images are shared more securely.
Sexual identity and life	Information relating to the individuals sexual life	☐ Yes ☑ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Family lifestyle and social circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐ Marital/partnership status ☐ Carers/relatives ☐ Children/dependents ☐ Social status e.g. housing ☑ Not applicable ☐ Other - please specify below: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Offences including alleged offences	Information relating to any offences committed or alleged to have been committed by the individual	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Criminal proceedings, outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education/training ☐ Qualifications ☐ Professional training ☑ Not applicable ☐ Other - please specify below: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Employment details	Employment and career history	☐ Employment status ☐ Career details ☑ Not applicable ☐ Other - please specify below: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Financial details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits ☑ Not applicable ☐ Other – please specify below: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☐ Yes ☑ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.
Trade union membership	Information relating to the individuals membership of a trade union	☐ Yes ☑ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	The change to process is around the transportation of photographic/video evidence and all personal details are removed.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it –if they are not you must amend the above selections to remove those items not relevant/necessary			
Confirm ☑			

Screen 6: Legal Basis for Processing the Data

Is the initiative delivering for Direct Care?

The definition of direct care is: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes:-

- *supporting individuals' ability to function and improve their participation in life and society*
- *the assurance of safe and high quality care and treatment through local audit,*
- *the management of untoward or adverse incidents*
- *person satisfaction including measurement of outcomes*

undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

☐ **Yes (go to Q2)** ☒ **No (go to Q1)**

1a. If not Direct care, what is it delivering and how is the consent being obtained	Indirect care • Commissioning ☐ • Monitoring Health and social care ☐ • Public health ☐ • Research ☐ • Other ☐ specify ……
1b. What is the legal basis that permits you to carry this out for indirect care?	Legal basis: • Explicit consent ☐ • Section 251 ☐ • Other legal gateway (please state) ☐ Previously discussed with the IG team who concluded that the organisation is to rely upon the category of 'legitimate interest of the data controller' as to obtain explicit consent would not be appropriate. This is because the implication of withdrawing or not giving consent to process data is that the request for funding couldn't be processed as a patient needs to be identified in order to gather the appropriate clinical information. Therefore this could be seen as being unfair as well as interrupting or delaying the process of handling a request which could have significant clinical consequences. This was approved at the GM EUR Steering Group in July 2018. The EUR Service is under a contractual obligation to provide the service to the 10 GM CCG's and it is the responsibility of the requestor to obtain explicit consent where appropriate.

2. What are the arrangements for individual's to either *object* to their information being shared for *direct care* or to *opt-out* of the initiative for *indirect care* once they have been provided with appropriate communication about it?	When a case is referred to a CCG IFR panel for consideration the clinician and patient are informed. An extract from the letter is below. If the PIA is approved then the extract will be amended (see changes in red): Current letter: **Information for the Patient:** Please note that in order for a decision to be made, your request and any associated further clinical information that we have collected is to be shared with the relevant CCG Individual Funding Panel members via secure post or email. In some instances your case may be discussed using Skype for Business Audio and Video Conferencing facility. We will only share the minimum information required for your request to be considered, and all information will be handled securely, confidentially and in accordance with the Data Protection Act 2018. If you object to us sharing your information you should contact us in writing to inform us immediately. However you should be aware that if you do not want this information to be shared with the relevant CCG panel members who are responsible for making a decision, then we may be unable to process your request for funding New letter: **Information for the Patient:** Please note that in order for a decision to be made, your request and any associated further clinical information that we have collected is to be shared with the relevant CCG Individual Funding Panel members via secure methods, including the transportation and sharing of any images that have been sent to us. In some instances your case may be discussed using Skype for Business Audio and Video Conferencing facility. We will only share the minimum information required for your request to be considered, and all information will be handled securely, confidentially and in accordance with the Data Protection Act 2018. If you object to us sharing your information (including electronic images if applicable) you should contact us in writing to inform us immediately. However you should be aware that if you do not want this information to be shared with the relevant CCG panel members who are responsible for making a decision, then we may be unable to process your request for funding

Informing individuals: How have patients and / or staff been informed of the data collection and processing?	Please state: No change to the way in which data is collected.

Information Sharing within UK:

Will personal confidential data be shared with any other organisation?

If yes, please state who the information will be shared with and how

☒ Yes ☐ No

From Originator Organisation:	Data sent to via:	To Receiving Organisation:
Clinicians involved in the patients care	The EUR Service via post or email	Greater Manchester CCG IFR Panels via secure links; secure emails or loaded securely on to approved laptops.
Patients and family members involved in the patients care	The EUR Service via post or email	Greater Manchester CCG IFR Panels via secure links; secure emails or loaded securely on to approved laptops.

Is the information from receiving organisation sent back to originating organisation. If yes, please state how the information is transferred back:

No – information is nor sent back; however a decision letter will be sent containing name, date of birth, NHS number, EUR teams unique reference number and the outcome. This letter will be sent via post and/or secure email.

From Receiving Organisation:	Data sent back via:	To originating organisation:

Information Sharing outside the UK:

Will Personal Confidential Data be sent outside the UK?

☐ Yes

☒ No

If yes, please state who the data will be sent to and how?

N/A

For the purposes of this PIA information is shared with Greater Manchester CCG's

Will Personal Confidential Data be sent outside the European Economic Area (EEA)?

☐ Yes

☒ No

If yes, please state who

the data will be sent to and how? Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security? If yes, please state what checks have been made: **Sending data to the USA**	N/A For the purposes of this PIA information is shared with Greater Manchester CCG's ☐ Yes ☒ No N/A For the purposes of this PIA information is shared with Greater Manchester CCG's ☐ Yes ☒ No

Screen 7: Asset / System Information

ICO Notification: If a system is being used, is the Supplier registered with the Information Commissioners Office (ICO). If yes, please state their registration number:	☐ Yes ☐ No N/A – this is a change to a process
IG Toolkit: Has the Supplier / Third party completed an Information Governance Toolkit Assessment & that has been internally/externally audited and/or has ISO27001 accreditation? If so, which version and to what level? Please provide evidence.	IG Toolkit completed: ☐ Yes ☐ No – N/A IG Toolkit audited ☐ Yes ☐ No – N/A ISO 27001 Accreditation ☐ Yes ☐ No – N/A Evidence: Click here to enter text.
Contract: Has the supplier (if applicable) signed the relevant contract (containing the Information Governance clauses) e.g. NHS E contract / SLA with IG Clause. If yes, please state which contract type they have signed up to:	☐ Yes ☐ No N/A this is a change to a process

Asset / System Operation: Does the asset use privacy invasive technologies for staff and / or patients? If yes, please state the technology being used: Will the asset / system process new / different personal confidential data items which have not been processed previously? If yes, please state the new personal confidential data items to be processed: **Data Subjects** Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients? If yes, please state the new identity authentication requirements: **Marketing:** Will the asset / system send marketing messages by electronic means? If yes, please state what you are intending to send for marketing purposes: Have individuals been informed of the marketing and the option to opt in?	Data Subjects ☐ Yes ☒ No N/A this is a change to a process ☐ Yes ☒ No ☐ Yes ☒ No Click here to enter text. ☐ Yes ☒ No Click here to enter text. ☐ Yes ☒ No – N/a

Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please describe this process and reason for it	☐ Yes ☒ No Click here to enter text.

Screen 8: System Security and Functions – only to be completed for systems

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☐ Yes ☒ No Any PID visible on images will be removed before being shared with a CCG IFR Panel or uploaded on to a laptop for viewing at a meeting.
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	N/A - the PIA is to request authorisation to change a process
Access: Who will have access to the system and the personal confidential data? How will levels of access be decided.	EUR Team. Access is removed and passwords are changed when staff leave the organisation
Auditing: Is there an audit trail for the system?	☒ No – N/A But the new process will be written into standard operating procedures which will inform staff that images/videos are removed from laptops immediately following a panel meeting.
Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☒ Within a system / application stored on secure network ☒ Within a database / spreadsheet stored securely on network ☒ Other — However copies of images will be removed from the laptop once they have been viewed. Originals will remain on the patient efile/database in line with NHS retention periods.
Retention: What are the retention periods for the information processed in the system?	NHS Records retention – 6 years. However images will be deleted from the laptop once viewed as these will be copies
Disposal: How will the personal	Deleted from the laptop

confidential data be disposed of when this is no longer required?	
Training: Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☒ Yes ☐ No

Screen 9: Additional Comments

Do you wish to supply additional comments about the system / asset? If yes please input comments in box:	☐ Yes ☒ No Click here to enter text.

Signed off by:

Organisation	Name	Date	Signature
GMSS	IG Group	21/11/2018	
Click here to enter text.	Click here to enter text.	Click here to enter a date.	

Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual which can be identified: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Sensitive Data	This means personal data consisting of information as to the: A) racial or ethnic group of the individual B) the political opinions of the individual C) the religious beliefs or other beliefs of a similar nature of the individual D) whether the individual is a member of a trade union E) physical or mental health of the individual F) sexual life of the individual G) the commission or alleged commission by the individual of any offence H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
Direct Marketing	This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation‟s information risk policy and acts as advocate for information risk on the Board

IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they „own" and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymity	This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic

	traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
Data Protection Act	This Act defines the way in which information about living people may be legally used and handled. The main intention is to protect individuals against misuse or abuse of information about them. This Act defines the way in which information about living people may be legally used and handled. The main intention is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: with those purposes loss, destruction or damage. unless that country or territory protects the rights and freedoms of the data subjects.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information. These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.