Greater Manchester Shared Services

Privacy Impact Assessment (PIA) Proforma

Reference: 00
PIA Title: [insert name]
Version: [insert version]
Date: [insert date]

DOCUMENT CONTROL PAGE	
Title	Privacy Impact Assessment Proforma
Version	2
Date	December 2015
Review	December 2017

Why do I need to complete a Privacy Impact Assessment?

Personal / sensitive data continues to be lost, inappropriately accessed and disposed of insecurely by third parties who public bodies have contracted services to. Therefore, the CCG / GMSS has to ensure that the third parties we process and share personal confidential data with, will ensure the data processed is undertaken securely and confidentially. To ensure this, we do a risk assessment called the Privacy Impact Assessment (PIA).

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.

This PIA is a shortened version of a longer template available on the ICO website and uses questions which are more suitable to the environment we work in.

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 using personal confidential data (PCD)
- 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

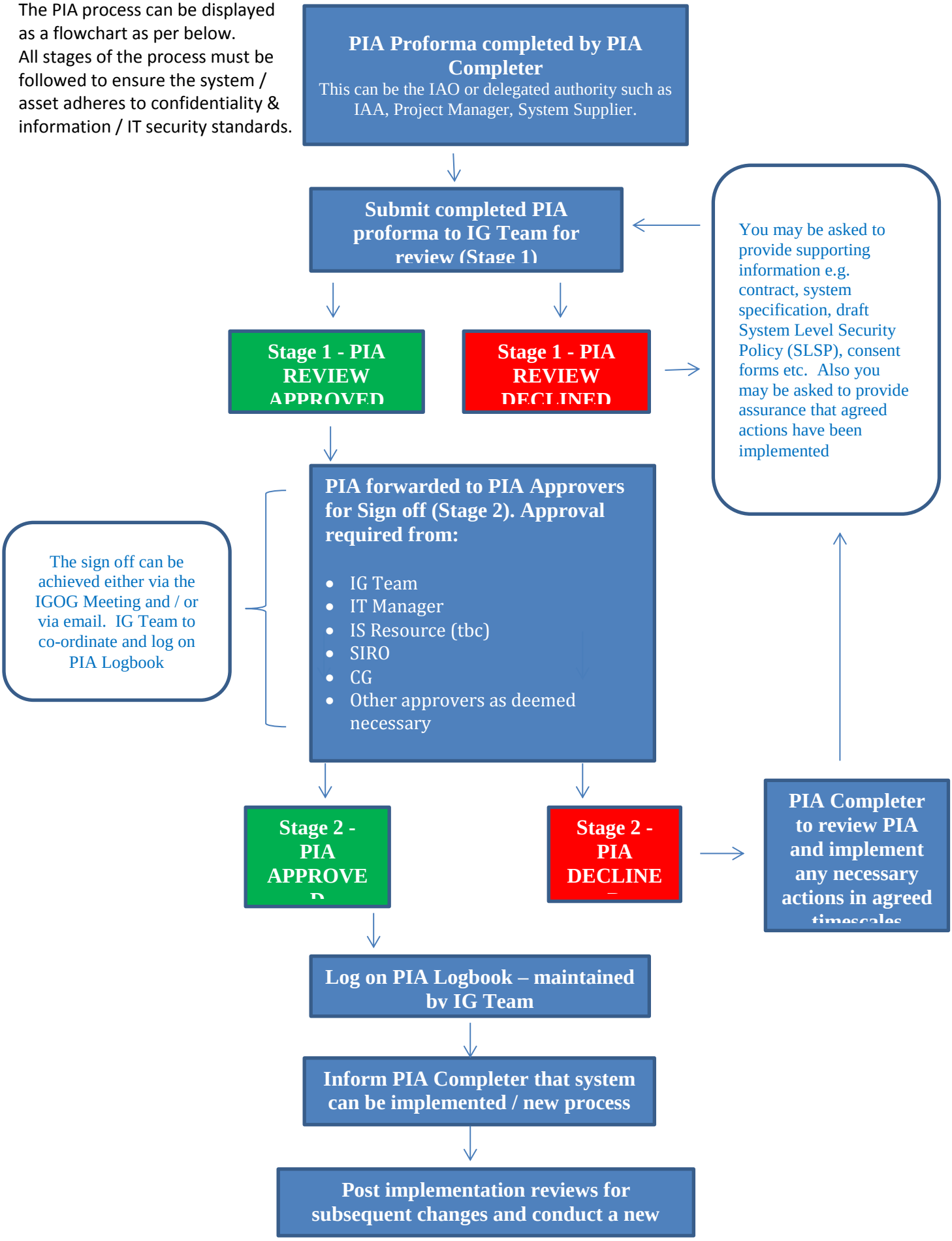
Please complete each section (where applicable) with as much information as possible. For example, a key piece of information is who the Information Asset Owner and Information Asset Administrator will be for a system / asset.

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: Basic Information

PIA Completer Name: *(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	Click here to enter text.
Department:	Click here to enter text.
Email:	Click here to enter text.
Telephone No.:	Click here to enter text.
New System / Process Name:	Click here to enter text.
New System Supplier Name: **(if applicable):**	Click here to enter text.
Date System due to go live (if applicable):	Click here to enter text.
Project Proposal / Purpose for completing PIA:	Click here to enter text.

Screen 2: Preliminaries

Will the system / process (referred to as 'asset') contain / use / process personal confidential data?	☐ Yes ☐ No

Screen 3: Contact Information

Project Management Details	
Project Manager:	Click here to enter text.
Project Manager Email:	Click here to enter text.
Project Manager Telephone No.:	Click here to enter text.
Information Asset Owner (IAO) Details	
IAO Name:	Click here to enter text.
IAO Title:	Click here to enter text.
IAO Department:	Click here to enter text.
IAO Email:	Click here to enter text.
IAO Telephone Number:	Click here to enter text.
Information Asset Administrator (IAA) Details	
IAA Name:	Click here to enter text.
IAA Title:	Click here to enter text.
IAA Department:	Click here to enter text.
IAA Email:	Click here to enter text.
IAA Telephone Number:	Click here to enter text.

Screen 4: Personal Confidential Data Items

Please tick below which of the personal and sensitive data items the asset / system will process.

Personal Data Items	Sensitive Data Items
☐ Forename(s) ☐ Surname ☐ Address ☐ Postcode ☐ Date of Birth ☐ Home Telephone Number ☐ Mobile Telephone Number ☐ Other Contact Number ☐ 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 state the 'Other' items in the box below Please list 'Other' personal data items to be processed: Click here to enter text.	☐ Gender ☐ Religion ☐ Ethnic Origin ☐ Medical Information ☐ Occupation / Employment ☐ Other Please list 'Other' sensitive data items to be processed: Click here to enter text.

Screen 5: Consent and Data Sharing

<table>
<tr><td>Informing individuals:

How have patients and / or staff been informed of the data collection and processing?</td><td>Please state:
Click here to enter text.</td></tr>
<tr><td>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

Is the information from receiving organisation sent back to originating organisation. If yes, please state how the information is transferred back:</td><td>☐ Yes

☐ No

<table>
<tr><td>From Originator Organisation:</td><td>Data sent to via:</td><td>To Receiving Organisation:</td></tr>
<tr><td>Click here to enter text.</td><td>Click here to enter text.</td><td>Click here to enter text.</td></tr>
<tr><td>Click here to enter text.</td><td>Click here to enter text.</td><td>Click here to enter text.</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td>From Receiving Organisation:</td><td>Data sent back via:</td><td>To originating organisation:</td></tr>
<tr><td>Click here to enter text.</td><td>Click here to enter text.</td><td>Click here to enter text.</td></tr>
<tr><td>Click here to enter text.</td><td>Click here to enter text.</td><td>Click here to enter text.</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

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?	..Click here to enter text.
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?	Click here to enter text.
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:	☐ Yes ☐ No
	Click here to enter text.
Sending data to the USA Is the country you are sending the Personal Confidential Data to a 'Safe Harbor' country?	☐ Yes ☐ No

Screen 6: 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 Click here to enter text.
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 IG Toolkit audited: ☐ Yes ☐ No ISO 27001 Accreditation: ☐ Yes ☐ No 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 Click here to enter text.

Asset / System Operation: Does the asset use privacy invasive technologies for staff and / or patients?	Staff ☐ Yes ☐ No Patients ☐ Yes ☐ No
If yes, please state the technology being used:	Click here to enter text.
Will the asset / system process new / different personal confidential data items which have not been processed previously?	☐ Yes ☐ No
If yes, please state the new personal confidential data items to be processed:	Click here to enter text.
Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients?	Staff ☐ Yes ☐ No Patients ☐ Yes ☐ No
If yes, please state the new identity authentication requirements:	Click here to enter text.
Marketing: Will the asset / system send marketing messages by electronic means?	☐ Yes ☐ No

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?	Click here to enter text. ☐ Yes ☐ No
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 7: 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
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	Click here to enter text.
Access: Who will have access to the system and the personal confidential data?	Click here to enter text.
Auditing: Is there an audit trail for the system?	☐ Yes ☐ No
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 Click here to enter text.

Retention: What are the retention periods for the information processed in the system?	Click here to enter text.
Disposal: How will the personal confidential data be disposed of when this is no longer required?	Click here to enter text.

Screen 8: 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.

Screen 9: Approval and Sign off

PIA Completed by:

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

Signed off by:

Organisation	Name	Date	Signature
Click here to enter text.	Click here to enter text.	Click here to enter a date.	
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 1998

This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state that personal data must be processed fairly and lawfully, be obtained only for lawful purposes and not processed in any manner incompatible with those purpose, be adequate, relevant and not excessive, be accurate and current, not be retained for longer than necessary, be processed in accordance with the rights and freedoms of data subjects, be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.

These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, emails and text. Unsolicited marketing material should only be sent if the

	requester has opted in to receive this information.
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.