

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	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.

PIA Proforma completed by PIA Completer
This can be the IAO or delegated authority such as IAA, Project Manager, System Supplier.

Submit completed PIA proforma to IG Team for review (Stage 1)

You may be asked to provide supporting information e.g. contract, system specification, draft System Level Security Policy (SLSP), consent forms etc. Also you may be asked to provide assurance that agreed actions have been implemented

Stage 1 - PIA REVIEW APPROVED

Stage 1 - PIA REVIEW DECLINED

PIA forwarded to PIA Approvers for Sign off (Stage 2). Approval required from:

- IG Team
- Other approvers as deemed necessary

The sign off can be achieved either via the IG Meeting and / or via email. IG Team to coordinate and log on PIA Logbook

Stage 2 - PIA APPROVED

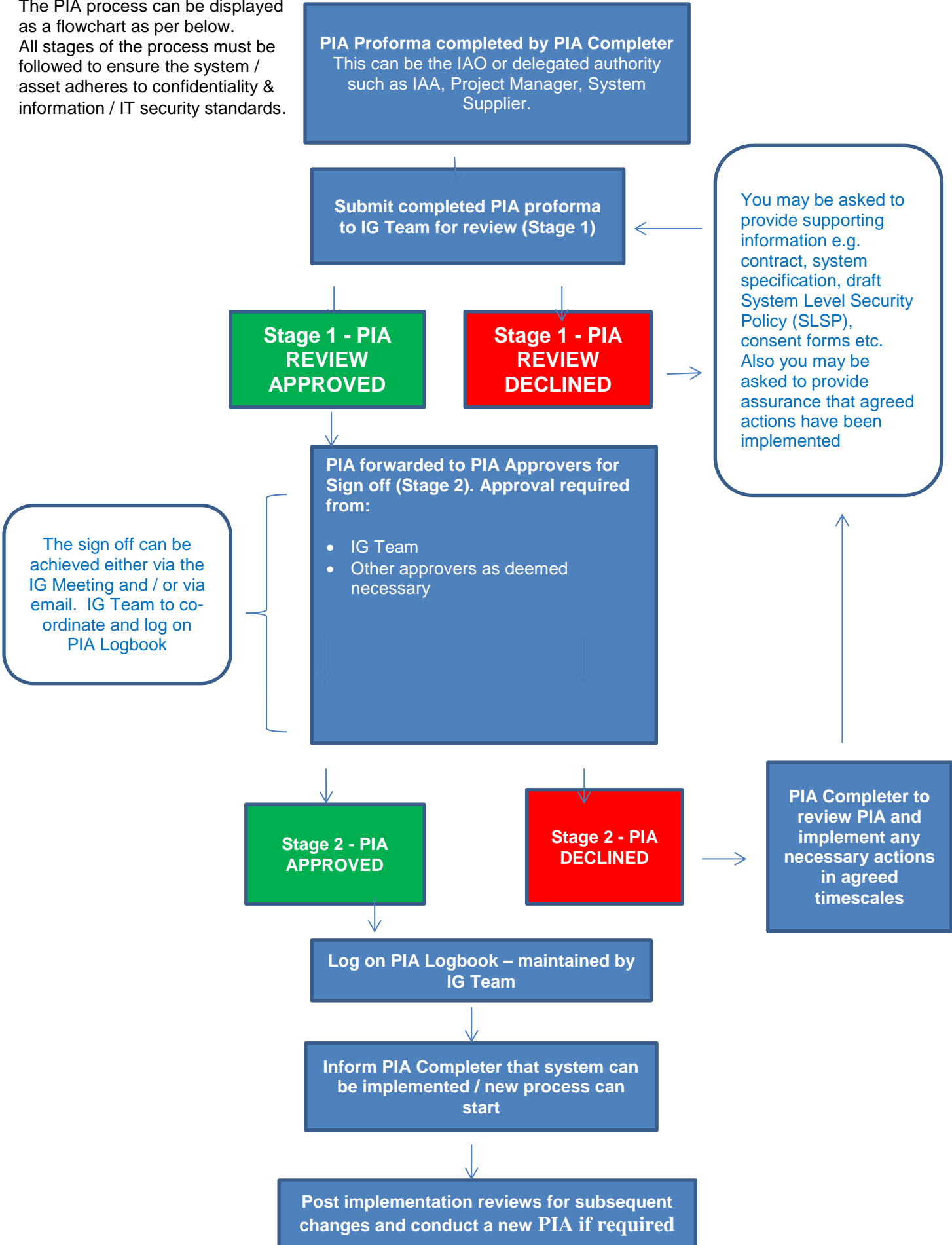
Stage 2 - PIA DECLINED

PIA Completer to review PIA and implement any necessary actions in agreed timescales

Log on PIA Logbook – maintained by IG Team

Inform PIA Completer that system can be implemented / new process can start

Post implementation reviews for subsequent changes and conduct a new PIA if required



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.	
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	<input type="checkbox"/>	Click here to enter a date.
Approved with action plan	<input type="checkbox"/>	Click here to enter a date.
Declined (give reason)	<input type="checkbox"/>	Click here to enter text. Click here to enter a date.

Screen 2: Basic Information

PIA Completer Name: <i>(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):</i>	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.
Link to any wider initiative: <i>(if applicable)</i>	Enter links to any wider initiatives if applicable
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
Are any other organisations are involved in this initiative?	[Click here to enter text.]		
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	
Is this initiative in line with or achieving national or local guidance/strategy or mandate?	If yes give details		

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 <i>Document initial comments on the issue and the privacy impacts or clarification why it is not an issue</i>
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Click here to enter text.
b)	Will the initiative involve the collection of new information about individuals?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Click here to enter text.
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Click here to enter text.]
d)	Will the initiative require you to contact individuals in ways which they may find intrusive ¹ ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Click here to enter text.]
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Click here to enter text.
f)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Click here to enter text.]
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Click here to enter text.
h)	Will the initiative compel individuals to provide information about themselves?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Click here to enter text.]

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 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 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 item(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: <ul style="list-style-type: none"> <input type="checkbox"/> Forename(s) <input type="checkbox"/> Surname <input type="checkbox"/> Address <input type="checkbox"/> Postcode <input type="checkbox"/> Date of Birth <input type="checkbox"/> Age <input type="checkbox"/> Gender <input type="checkbox"/> Physical description <input type="checkbox"/> Home Telephone Number <input type="checkbox"/> Mobile Telephone Number <input type="checkbox"/> Other Contact Number <input type="checkbox"/> Email address <input type="checkbox"/> GP Name and Address <input type="checkbox"/> Legal Representative Name (Next of Kin) <input type="checkbox"/> NHS Number <input type="checkbox"/> National Insurance Number <input type="checkbox"/> Photographs/Pictures of persons <input type="checkbox"/> Other – if this is ticked please list 'Other' personal data items to be processed below: See attached	Click here to enter text.
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	<ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	Click here to enter text.

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.		
Sexual identity and life	Information relating to the individuals sexual life	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	Click here to enter text.
Family lifestyle and social circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	<input type="checkbox"/> Marital/partnership status <input type="checkbox"/> Carers/relatives <input type="checkbox"/> Children/dependents <input type="checkbox"/> Social status e.g. housing <input type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below: [Click here to enter text.]	[Click here to enter text.]
Offences including alleged offences	Information relating to any offences committed or alleged to have been committed by the individual	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	Click here to enter text.
Criminal proceedings, outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	[Click here to enter text.]
Education and training details	Information which relates to the education and any professional	<input type="checkbox"/> Education/training <input type="checkbox"/> Qualifications	[Click here to enter text.]

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
	training of the individual	<input type="checkbox"/> Professional training <input type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below: [Click here to enter text.]	
Employment details	Employment and career history	<input type="checkbox"/> Employment status <input type="checkbox"/> Career details <input type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below: [Click here to enter text.]	[Click here to enter text.]
Financial details	Information relating to the financial affairs of the individual	<input type="checkbox"/> Income <input type="checkbox"/> Salary <input type="checkbox"/> Benefits <input type="checkbox"/> Not applicable <input type="checkbox"/> Other – please specify below: [Click here to enter text.]	Click here to enter text.
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	Click here to enter text.
Trade union membership	Information relating to the individuals membership of a trade union	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix: [Click here to enter text.]	[Click here to enter text.]

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)

<p>1a. If not Direct care, what is it delivering and how is the consent being obtained</p>	<p>Indirect care</p> <ul style="list-style-type: none"> • Commissioning <input type="checkbox"/> • Monitoring Health and social care <input type="checkbox"/> • Public health <input type="checkbox"/> • Research <input type="checkbox"/> • Other <input type="checkbox"/> specify
<p>1b. What is the legal basis that permits you to carry this out for indirect care?</p>	<p>Legal basis:</p> <ul style="list-style-type: none"> • Explicit consent <input type="checkbox"/> • Section 251 <input type="checkbox"/> • Other legal gateway (please state) <input type="checkbox"/> <p>[Click here to enter text.]</p>
<p>2. What are the arrangements for individual's to either <u>object</u> to their information being shared for <u>direct care</u> or to <u>opt-out</u> of the initiative for <u>indirect care</u> once they have been provided with appropriate communication about it?</p>	<p>[Click here to enter text.]</p>

<p>Informing individuals:</p> <p>How have patients and / or staff been informed of the data collection and processing?</p>	<p>Please state:</p> <div style="border: 1px solid black; height: 60px; width: 100%;"></div>

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:

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

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

Information Sharing outside the UK:

Will Personal Confidential Data be sent outside the UK?

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

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

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

Yes

No

Yes

No

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

Sending data to the USA

Yes

No

Screen 7: Asset / System Information

<p>ICO Notification:</p> <p>If a system is being used, is the Supplier registered with the Information Commissioners Office (ICO).</p> <p>If yes, please state their registration number:</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <div data-bbox="517 501 1209 568" style="border: 1px solid black; height: 30px; width: 434px;"></div>
<p>IG Toolkit:</p> <p>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?</p> <p>Please provide evidence.</p>	<p>IG Toolkit completed:</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>IG Toolkit audited</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>ISO 27001 Accreditation</p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <p>Evidence: Click here to enter text.</p>
<p>Contract:</p> <p>Has the supplier (if applicable) signed the relevant contract (containing the Information Governance clauses) e.g. NHS E contract / SLA with IG Clause.</p> <p>If yes, please state which contract type they have signed up to:</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <div data-bbox="517 1724 1382 1841" style="border: 1px solid black; padding: 5px;"><p>Click here to enter text.</p></div>

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:

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

Click here to enter text.

Yes

No

Click here to enter text.

Data Subjects

Yes

No

Click here to enter text.

Yes

No

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

<p>Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?</p>	<p>Click here to enter text.</p>
<p>Access: Who will have access to the system and the personal confidential data? How will levels of access be decided.</p>	<p>Click here to enter text.</p>
<p>Auditing: Is there an audit trail for the system?</p>	<p><input type="checkbox"/> No</p>
<p>Storage of data: Where will the system information be stored securely?</p>	<p><input type="checkbox"/> Within a paper based system stored securely</p> <p><input type="checkbox"/> Within a system / application stored on secure network</p> <p><input type="checkbox"/> Within a database / spreadsheet stored securely on network</p> <p><input type="checkbox"/> Other <input type="text" value="Click here to enter text."/></p>
<p>Retention: What are the retention periods for the information processed in the system?</p>	<p>Click here to enter text.</p>
<p>Disposal: How will the personal confidential data be disposed of when this is no longer required?</p>	<p>Click here to enter text.</p>

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

<p>Do you wish to supply additional comments about the system / asset?</p> <p>If yes please input comments in box:</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Click here to enter text.</div>
--	--

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 organisations which provide information to individuals may be legally used. It may be legally used to protect individuals against fraud, to be a source of information for individuals. The 8 principles of the Act state that use of information must be lawful, be obtained lawfully, be adequate, relevant and not excessive, be processed in accordance with the rights and freedoms of individuals, be processed in accordance with the rights and freedoms of individuals, be processed in accordance with the rights and freedoms of individuals, be processed in accordance with the rights and freedoms of individuals. The 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.

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.

