
Data Protection Impact Assessment Procedure and Proforma

Version:	5.0
Ratified by:	NHS Bury CCG Information Governance Operational Group
Date ratified:	18 June 2021
Name of originator /author (s):	GMSS IG Team
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	July 2021
Review date:	March 2023
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Data Privacy Impact Assessment Procedure and Proforma CCG.GOV.027.5.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS IG Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff.
This document has been developed in consultation with	NHS Bury CCG Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 3100
Copies of this document are available from	CCG Corporate Office CCG Website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
2.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	27 th November 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	18 th November 2015
3.1 = policy review	GMSS IG Team	5 th March 2018
4.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	26 th March 2018
4.1 = review	NHS Bury Clinical Commissioning Group, Information Governance Team	15 th June 2021
5.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	18 th June 2021

Data Privacy Impact Assessment Proforma

Why do I need to complete a Data 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 DPIA 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.

When do I complete a Data Protection Impact Assessment?

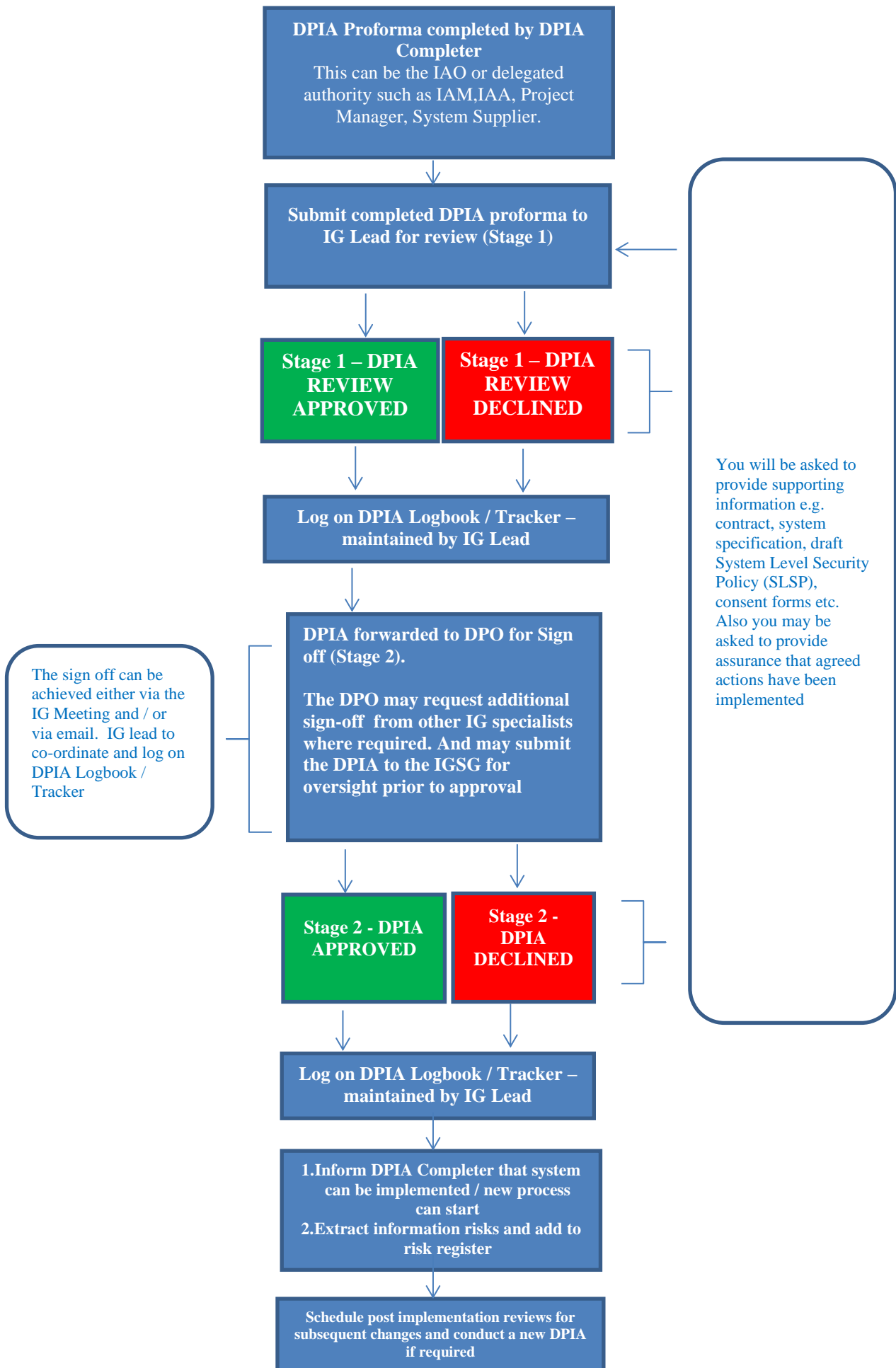
If you are doing any of the following:

- 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

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

Who needs to complete a Data Privacy Impact Assessment (DPIA)?

It is the Information Asset Owners responsibility to ensure that a DPIA is completed and submitted to the IG Team for review. A DPIA can be delegated to an Information Asset Manager (IAM), Information Asset Administrator (IAA), a Project Manager and / or a suppliers of a system or information asset, where they are the most appropriate person to complete the document.



Important

By completing this Data Privacy Impact Assessment, you agree to adhere to the Data Security and Protection Toolkit requirements and have Information Governance and Information Security Policies in place which includes:

- Information Governance Policy
- Completion of Information Governance Mandatory Training
- Information Governance Incident Reporting Procedures
- Secure 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).

Help and Advice

Further advice and guidance on how to complete this form can be obtained from the IG Manager.

Section 1: Basic Information

Reference:	XXXXXXXXXX
DPIA Title:	XXXXXXXXXX

DPIA Completer Name: <i>(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):</i>	
Department:	
Email:	
Telephone No.:	
New System / Process Name:	
New System Supplier Name: (if applicable):	
Date System due to go live (if applicable):	
Project Proposal / Purpose for completing DPIA:	
Link to wider initiative <i>(if applicable):</i>	
Information Technology Involvement	
Are any other organisations involved in this initiative?	

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?		

Section 2: Screening Questions

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"/>	
b)	Will the initiative involve the collection of new information about individuals?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
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"/>	
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"/>	
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"/>	
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"/>	
h)	Will the initiative compel individuals to provide information about themselves?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

If you answered **YES** or **UNSURE** to any of the above you need to continue with the data protection impact assessment.

Sign off if no requirement to continue with Data Protection Impact Assessment:
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the data protection impact assessment
Agreed by: <input type="text" value="Click here to enter name of group or individual(s)."/>

Section 3: Contact Information

Project Management Details	
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:	

Section 4: 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	<p>Check all that apply:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Forename(s) <input checked="" type="checkbox"/> Surname <input checked="" type="checkbox"/> Address <input checked="" type="checkbox"/> Postcode <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Age <input checked="" type="checkbox"/> Gender <input checked="" type="checkbox"/> Physical description <input checked="" type="checkbox"/> Home Telephone Number <input checked="" type="checkbox"/> Mobile Telephone Number <input checked="" type="checkbox"/> Other Contact Number <input type="checkbox"/> Email address <input checked="" type="checkbox"/> GP Name and Address <input checked="" type="checkbox"/> Legal Representative Name (Next of Kin) <input checked="" type="checkbox"/> NHS Number <input type="checkbox"/> National Insurance Number <input checked="" type="checkbox"/> Photographs/Pictures of persons <input type="checkbox"/> Other – if this is ticked please list 'Other' personal data items to be processed below: <p>For specific details see the MIG Content Model record elements and read code mapping document v2.03 July 2017.</p>	

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
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 Mental Health Act.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not applicable	
Sexual Identity and Life	Information relating to the individuals sexual life	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Not applicable	
Family Lifestyle and Social Circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	<input checked="" type="checkbox"/> Marital/partnership status <input checked="" type="checkbox"/> Carers/relatives <input checked="" type="checkbox"/> Children/dependents <input checked="" type="checkbox"/> Social status e.g. housing <input type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below:	
Offences including Alleged Offences	Information relating to any offences committed or alleged to have been committed by the individual	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix:	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
Criminal Proceedings, Outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Not applicable List any data items below or attach as an appendix:	[Click here to enter text.]
Education and training details	Information which relates to the education and any professional training of the individual	<input type="checkbox"/> Education/training <input type="checkbox"/> Qualifications <input type="checkbox"/> Professional training <input checked="" type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below:	
Employment details	Employment and career history	<input type="checkbox"/> Employment status <input type="checkbox"/> Career details <input checked="" type="checkbox"/> Not applicable <input type="checkbox"/> Other - please specify below:	
Financial details	Information relating to the financial affairs of the individual	<input type="checkbox"/> Income <input type="checkbox"/> Salary <input type="checkbox"/> Benefits <input checked="" type="checkbox"/> Not applicable <input type="checkbox"/> Other – please specify below:	
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	

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
		<input type="checkbox"/> Not applicable List any data items below or attach as an appendix:	
Trade union membership	Information relating to the individuals membership of a trade union	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
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 <input checked="" type="checkbox"/>			

Section 5: Data Flows

It is essential that each flow of data is identified, documented and specifies the security measures in place. *NB. Even if the data is only being viewed in a system it is a flow of data and should be included.*

These must be transferred onto your service's data flow mapping.

Flow Ref	Flow name/ description	Going from	Going to	Method of access/transfer and control	Specify the security control(s) in place for the flow	Where will the data be stored after access/transfer?
<i>Example01</i>	<i>Notification of referral letter</i>	<i>Rapid Response Team / Paris</i>	<i>GP</i>	<i>External post</i>	<i>SOP developed and agreed outlining process for letters; staff will receive regular 1:1s and clinical supervision; letters created and stored within Paris with access controls in place</i>	<i>None of the above</i>

Section 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>1b. What is the legal basis that permits you to carry this out for indirect care?</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>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>
--	--

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>Informing individuals: Please state how patients and / or staff will be informed / have been informed of the data collection and processing?</p>																									
<p>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 and enter in the table:</p> <p>Is the information from receiving organisation sent back to originating organisation? If yes, please state how the information is transferred back and enter in the table:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">From Originator Organisation:</th> <th style="width: 33%;">Data sent to via:</th> <th style="width: 33%;">To Receiving Organisation:</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">From Receiving Organisation:</th> <th style="width: 33%;">Data sent back via:</th> <th style="width: 33%;">To Originating Organisation:</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>	From Originator Organisation:	Data sent to via:	To Receiving Organisation:										From Receiving Organisation:	Data sent back via:	To Originating Organisation:									
From Originator Organisation:	Data sent to via:	To Receiving Organisation:																							
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?

..

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

- Yes
- No
- Not Applicable

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 standards in place? If yes, please state what checks have been made:

- Yes
- No
- Not applicable

|

Sending data to the USA?

- Yes
- No
- Not Applicable

Section 7: Asset / System Information

<p>ICO Notification: If a system is being used, is the Supplier (of this system) registered with the Information Commissioners Office (ICO).</p> <p>If yes, please state their registration number:</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable (Please specify reason: _____)</p> <p>Registration No:</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable (Please specify reason: _____)</p> <p>Registration No:</p>		
<p>DSP Toolkit: Has the Supplier / Third party completed a Data Security & Protection Toolkit Assessment (formerly IG Toolkit) and / or had a ISO27001 accreditation?</p> <p>As regards the DSP Toolkit, please state which version was submitted and if this achieved a satisfactory or non-satisfactory status?</p>	<p>DSP Toolkit completed: <input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>DSP Toolkit audited <input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>ISO 27001 Accreditation <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>ISO27001 certification number –</p> <p><i>Version:</i></p>
<p>Contract: Has the third party 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 checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>		

Asset / System Operation:

Does the asset use privacy invasive technologies for staff and / or patients, e.g. Smartcards?

- Yes
- No

If yes, please state the technology being used:

Will the asset / system process 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:

Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients?

- Yes
- No

If yes, please state the new identity authentication requirements:

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:

- Yes
- No

Have individuals been informed of the marketing and the option to opt in to this?

Automated Decision Making:

Is automated decision making to be used within the asset / system?

- Yes
- No

If yes, please briefly describe the process and the reason for it?

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

<p>Pseudonymisation / Anonymisation:</p> <p>Can personal confidential data be anonymised or pseudonymised using the system / asset?</p>	<p><input type="checkbox"/> Yes</p> <p><input checked="" type="checkbox"/> No</p>
<p>Data Quality:</p> <p>How will the personal confidential data be kept up to date and checked for accuracy?</p>	
<p>Access:</p> <p>Who will have access to the system and the personal confidential data? How will access be controlled?</p>	
<p>Auditing:</p> <p>Is there an audit trail for the system?</p> <p>Please can you describe briefly how the audit trail works?</p>	<p><input checked="" type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Storage of data:</p> <p>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 checked="" type="checkbox"/> Other</p>
<p>Back Up:</p>	

<p><u>Applicable for IT systems only:</u> Are there secure and reliable back up processes in place for the data stored on the system?</p> <p>If yes, please briefly describe what these are. <i>Please note you may need to contact IT Services for guidance regarding this question</i></p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;">N/A</div>
<p>Retention: Please state the retention periods for the information processed in the system? <i>Please refer to the Records Management: NHS Code of Practice for Health & Social Care 2016 for assistance with this</i></p>	<p>N/A</p>
<p>Disposal: How will the personal confidential data be disposed of when this is no longer required.</p>	<p>N/A</p>
<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</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>It is a requirement within the ISA with partner organisations that staff with access will have completed there mandatory IG training</p>

Section 9: Business Continuity

Do you have a Business Continuity Plan in place if the system and / or process fail or is unavailable for any reason?

If yes, briefly describe what the business continuity plan will be in the box:

- Yes
 No

Section 10: Additional Comments

Do you wish to supply additional comments about the system / asset?

- Yes
- No

If yes please input comments in box:

Section 11: Risks and Privacy Issues

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- unauthorised access to data
- undesired modification of data
- disappearance of data
- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

Include any sources of the risk i.e. person or non-human source that can cause a risk either accidentally or deliberately:

The risks should be reviewed, scored using the risk matrix below and incorporated into a risk register. The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then multiplied to create the composite risk score using the risk matrix below. This should be recalculated in the final columns to take into account proposed solutions/actions/mitigations.

Risk	Detail	Risk Level			Mitigation	Owner	Target Risk Level			Next Review Date
		C	L	R			C	L	R	

Consequence (How bad it may be)		Likelihood (The chance it may occur)		Risk Rating <i>Likelihood x Impact = TOTAL RISK RATING</i>					
				Impact					
				1	2	3	4	5	
5	Very High <i>(Will have a major impact)</i>	5	Almost certain <i>(almost certain to happen/recur; possibly frequently)</i>	Likelihood	5	10	15	20	25
4	Major <i>(highly probable it will have a significant impact)</i>	4	Likely <i>(Will probably happen/recur, but is not a persisting issue or circumstance)</i>		4	8	12	16	20
3	Moderate <i>(Likely to have an impact)</i>	3	Possible <i>(Might happen or recur occasionally)</i>		3	6	9	12	15
2	Minor <i>(May have an impact)</i>	2	Unlikely <i>(Do not expect it to happen/recur, but it is possible it may do so)</i>		2	4	6	8	10
1	Negligible <i>(Unlikely to have any impact)</i>	1	Rare <i>(This probably will never happen/recur)</i>		1	2	3	4	5

Total Risk Rating	Risk
1-3	Low
4-6	Moderate
8-12	High
15-25	Extreme

DPIA Completed by:

Organisation	Name	Date	Signature

Section 12: Assurance Review

Information Governance Review Specify any issues identified, recommendations and actions needed to secure the data if appropriate controls not in place within the risk assessment:			Project Response	
Issue and section no. of DPIA where this was identified	Potential risk	Recommendation	Agreed action	Accountable lead and completion date

Information Governance Review of Risks	<input type="checkbox"/> No risks identified <input type="checkbox"/> All privacy risks have been identified and actions are underway to mitigate, accept or remove the risks. This action plan will now be reviewed and monitored via _____ <input type="checkbox"/> All privacy risks have been identified and actions completed to mitigate, accept or remove the risks <input type="checkbox"/> Not all privacy risks can be removed or reduced and the processing remains high risk, therefore the ICO must be consulted
ICO Review required <i>Where the processing remains high risk, that cannot be mitigated or remove, the ICO must be consulted</i>	<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, ICO review outcome and date:	

Information Asset Management Assurances

Data flows incorporated into data flow mapping	<input type="checkbox"/>	
Assets incorporated into the asset register	<input type="checkbox"/>	
Confirm staff handling subject access requests are aware of new or changed information asset	Yes <input type="checkbox"/> Not applicable <input type="checkbox"/>	
Confirm Information Sharing arrangements documented: <ul style="list-style-type: none"> • within this DPIA, and ISA not required <input type="checkbox"/> • within a separate IS agreement <input type="checkbox"/> • planned within the DPIA action plan <input type="checkbox"/> • Within a Data processing contract <input type="checkbox"/> Other: specify -		
Monitor and review of this DPIA	Who by:	When:

For IG use only

Action	Confirm	Date
Data Protection officer (DPO) review	<input type="checkbox"/>	
DPO review not required	<input type="checkbox"/>	Decision made by:
IG significant assurance – no actions required	<input type="checkbox"/>	
IG limited assurance – action plan required	<input type="checkbox"/>	
Declined (give reason)	<input type="checkbox"/>	

Section 13: Approval

Approved by:

Organisation	Name	Date	Signature

APPENDIX 1: List of names and job roles who will be accessing systems

Name	Role	Organisation	Name of System	Access level Read only / Read and write	IG training completed date (must be within 12 months)

APPENDIX 2: Legal basis for sharing.

- The following are categorised as special category data: race, ethnic origin politics religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation. As such it must meet at least one basis in Article 6 **and** one from Article 9.

Article 6 (1)

- a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 9

- a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes
- b) processing is necessary for the purposes of carrying out the obligations and exercising specific **rights of the controller or of the data subject in the field of employment and social security** and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- d) processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it

in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- e) processing relates to personal data which are manifestly made **public by the data subject**;
- f) processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity;
- g) processing **is necessary for reasons of substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- h) processing is necessary for the purposes of **preventive or occupational medicine**, for the **assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- i) processing is necessary for reasons of **public interest** in the area of **public health, such as protecting against serious cross-border** threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- j) processing is necessary for **archiving purposes** in the **public interest, 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 to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

APPENDIX 3: Glossary of Terms

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.