

Status:	Approved <input type="checkbox"/>
	Approved with Actions <input type="checkbox"/>
	Not Approved <input type="checkbox"/>
Purpose of Completion:	New System/Service/Device <input type="checkbox"/>
	Contract Renewal <input type="checkbox"/>
	Review/Change in process <input type="checkbox"/>
	Approved Actions Follow up <input type="checkbox"/>

Data Protection Impact Assessment

(DPIA)

Article 35(1) of the General Data Protection Regulations says that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals:

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”

Initiative/System/Process name:	
Projected Go-Live Date	
Date DPIA commenced:	
Is this a new project?	Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, has this been developed by an individual or an associate of an individual who works for UHNM? Yes <input type="checkbox"/> No <input type="checkbox"/> Please give details-
Is this a project directed by a Trust Executive?	Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, please give details:
Capital Bid	Reference No. Over £20K Yes <input type="checkbox"/> No <input type="checkbox"/>
ERCAF Reference Number	
DPIA Reference Number	

Document Version Control

Version	Issue Date	Comments
1		
2		
3		
4		

DPIA Template Version History:

Version	Date	Updated By	Amendment/s
1	23.4.20	Rachel Montinaro	New DPIA template. Approved and issued May 2020
2	16.07.20	Rachel Montinaro	Added New project question, reference to the DPA and national guidance reference
3	12.08.20	Rachel Montinaro	Risk Assessment document display method changed
4	19.10.20	Rachel Montinaro	Question 1.1.10 audit question added, Action plan and EREAF ref number added
5	27/10/2020	Marsha Walker/Rachel Montinaro	Replaced risk table to resolve over writing issue, EREAF and capital bid questions added. Executive board member question added
6	15/12/20	Rachel Montinaro	Added GDPR table, SCCs link and included questions 1.6.3 1.6.4 and 1.6.5, ODS reference added. Approval table added
7	04/05/21	Rachel Montinaro	Supplier assurances and additional evidence question 1.7.2 Asset Owner/administrator questions added
8	15.06.21	Rachel Montinaro	Question 1.1.12 added to ask if under 18's data is used Question 1.7.7 automated decision making added
9	16.06.22	Rachel Montinaro	Guidance added for AI and profiling
10	16.08.22	Stuart Goodwin	Questions 1.1.3, 1.1.4, 1.1.5, 1.7.2, 1.7.3 & 1.7.4 added. DPA Schedule 1 special category legal basis added.
11	15.02.23	Stuart Goodwin/Rachel Montinaro	Removed SCCs link, Questions 1.1.11, 1.1.14, 1.1.15, 1.1.16 reworked, Question 1.7.7, 1.7.8, 1.7.9 & automated processing included in question 1.1.16. Question 1.3.3 removed. Questions 1.5.1 & 1.5.2 reworked. Question 1.6.2 added Questions 1.6.3, 1.6.4, 1.6.5 & 1.6.6 included in question 1.6.3 Question 1.7.2 link to ICO & DSP toolkit search added Section 5 Risk Assessment guidance included as a word document Consent questions added
12	16.06.23	Stuart Goodwin	Added Purpose of Completion checkbox, Updated dropdown lists in Dataflow
13	26.06.23	Stuart Goodwin	Question 1.6.3 updated to include PACs integration
14	14.09.23	Stuart Goodwin	Link to retention schedule 1.5.1 updated to 2023 schedule
15	05.10.23	Stuart Goodwin	Questions 1.6.2 & 1.6.3 added to cover multi factor authentication (MFA), subsequent questions 1.6.4 -1.6.10 re-numbered Question 1.7.2 added to request contract expiry date Question 1.6.5 updated to reword question Question 1.6.4 updated to include RBAC
16	24.06.24	Stuart Goodwin	Document Version Control added to page 1 to document changes made to the completed DPIA. Link to Human Rights Act 1998 - Article 8 definition on page 3 updated. Questions 1.6.2 & 1.6.3 reworked to cover Trust's multi factor authentication (MFA) Questions 1.6.4 & 1.6.5 added to confirm authentication factors used and available. Question 1.1.16 updated to cover use of Artificial Intelligence (Ai)

The DPIA Process

The Data Protection Act is mainly concerned with the disclosure of personal data outside the data controller's own boundaries.

- 1) Please complete each section with as much detail as possible and your DSP lead can assist you.
- 2) Once you submit the DPIA for approval to/via your Data Security and Protection Lead/Data Protection Officer (DPO)
- 3) The DPIA proforma will be vetted and you may receive some comments / questions asking for further information. Please answer these promptly and resend the DPIA again. .


- 4) The DPIA then goes for approval. It is considered for approval by the relevant DSP internal approval process.
- 5) Once approved, the process / system can start to be introduced or modification to an existing system / process can continue.
- 6) If you proceed with the initiative without completing the DPIA and without approval via the DSP DPIA approval process, you are putting the organisation at risk of being in breach of the DP legislation which may result in disciplinary procedures being invoked.

DPIA Contact Details: Please list all main contributors in completing the DPIA				
Name	Role	Organisation/Department	Email	Telephone Number

Who will be the Asset Owner once this system/asset has gone live?

Who will be the Asset Administrator once this system/asset has gone live?

Legal powers – There must be a statute in law which allows you to conduct business – for the NHS it will be the NHS Act; Health & Social Care Act. It is also necessary that you identify that you have taken account of the Common Law Duty of Confidentiality as well as the Human Rights Act (1998).

Common Law duty of confidentiality	Human Rights Act 1998 - Article 8	Legal powers/vires Data Protection Act 2018 – principle 1	DPA SCHEDULE 1
<p><i>NB. Consent can be implied for the purposes of direct care. Where the whole/entire patient record is being shared explicit consent should be sought as per BMA and National Data Guardian guidance (sec 1.32).</i></p> <p><i>The definition of direct care is¹: 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:-</i></p> <ul style="list-style-type: none"> • 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 	<p>1998 - Article 8 - See <i>Human Rights: Human Lives Equality and Human Rights Commission - A Guide to the Human Rights Act for Public Authorities</i></p> <p>Article 8: Respect for your private and family life EHRC (equalityhumanrights.com)</p> <p style="text-align: center;">Is there any interference with Human Rights Article 8? If yes, document why it is necessary and proportionate to do so:</p>	<p>What are the organisations legal powers to process the information?</p> <div style="text-align: center;">  COEIS_Process-for-deciding-the-legal-basis </div>	<p>Special categories of personal data.</p> <p>Provides a list of conditions which, if one is met, permit the processing of the special categories of personal data.</p> <p>Details policy documentation and additional safeguards which must be put in place when relying on some of the conditions listed.</p> <p>These apply to the UK GDPR and applied UK GDPR.</p>

<input type="checkbox"/> Explicit consent <input type="checkbox"/> Implied consent <input type="checkbox"/> Public Interest or safeguarding individual/other <input type="checkbox"/> Legal Duty <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know – seek advice from DSP	<input type="checkbox"/> NHS Act 2006 <input type="checkbox"/> Health and Social Care Act 2012 <input type="checkbox"/> Local Authority <input type="checkbox"/> Other Public Sector <input type="checkbox"/> Private and 3 rd sector (see PDF above) <input type="checkbox"/> Data Protection Act 2018 <input type="checkbox"/> Other (details to be provided e.g. GDPR Recital 52– stating ‘Such a derogation may be made for health purposes, including public health and the management of health-care services’ as it will be used for the review/evaluation of services.)	Part 1 Conditions related to Employment, Health and Research <input type="checkbox"/> Employment, social security and social protection <input type="checkbox"/> Health or social care purposes <input type="checkbox"/> Public health <input type="checkbox"/> Research
---	---	--	---

Section 1: Project Information

Lawfulness, fairness and transparency - Article 5(1)(a) of the GDPR says: “1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness, transparency’)”

- You must identify valid grounds under the GDPR (known as a ‘lawful basis’) for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

Caldicott Principle 1: Justify the purpose for using confidential information

Caldicott Principle 6: Understand and comply with the law

Project Description – A summary of the project and the aims	
1.1.1	

How long do you expect this initiative to last?	
1.1.2	End of contract <input type="checkbox"/> Specific time period <input type="checkbox"/> -specify Lifetime of system <input type="checkbox"/> Other <input type="checkbox"/> - specify

Does the system need to be recorded on the Information Asset Register?
--

1.1.3	Yes <input type="checkbox"/> No <input type="checkbox"/> Medical Device <input type="checkbox"/> Don't Know <input type="checkbox"/>
-------	--

If an Information Asset, what classification will the Asset be recorded as?

1.1.4	<p>Priority 1 A - A system that is critical for patient care: (i.e. emergency care, diagnostic) <input type="checkbox"/></p> <p>Priority 1 B - A system that is critical for patient care: (i.e. emergency admission, monitoring, 7/7 service) <input type="checkbox"/></p> <p>Priority 1 C - A system that is critical for patient care: (i.e. outpatient, elective admission, core business hours) <input type="checkbox"/></p> <p>Priority 2 - A system that is used for patient registration, communication and affects the Hospital financially or reputationally <input type="checkbox"/></p> <p>Priority 3 - A system that adds efficiencies <input type="checkbox"/></p> <p>N/A <input type="checkbox"/></p>
-------	---

Is this system/app used by patients?

1.1.5	Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>
-------	---

Does this project have any links or references to national guidance? Please evidence

1.1.6	<i>e.g. ICO/NHSx</i>
-------	----------------------

What stage is the project currently at?

1.1.7	
-------	--

Which divisional groups has this project been tabled for discussion and approval, when?

1.1.8	
-------	--

**What information will be collected, processed, accessed and stored?
Please include the data set**

1.1.9	
-------	--

Is the data already captured by the Trust for this purpose?

1.1.10	Yes <input type="checkbox"/> No <input type="checkbox"/>
--------	--

Describe the nature of the processing, how will you collect, use and store data?

Please include information to cover:

- *What is the source of the data? i.e. is this via a system feed or manual data entry*
- *Once collected how will the data be used and for what purpose*
- *Will the data be sent to another system? If so how will this be transferred*
- *Will you be sharing data with anyone? If so what method will be used to transfer the data*
- *Where will the data be stored? i.e. will this be on the Trust network or an external cloud*

You might find it useful to refer to a flow diagram or other way of describing data flows.

1.1.11

How often will you be collecting and using the personal data?

1.1.12

How often will the new system, process or data flow be audited? *Each partner organisation should have a programme of audit in place for their respective systems that tests for patterns of access, inappropriate access etc. that is routinely undertaken.*

1.1.13

Approximately how many data subjects will this process involve?

1.1.14

- 0-50
- 50-500
- 500-1000
- 1000+

Does this system/service contain data relating to sensitive cohorts of data subjects?

1.1.15

- Under 18's
- Gender
- Adoption
- No

Individual Rights

How are data subjects informed of the processing? What information are they provided with? Please provide the Patient leaflet, consent form and link to privacy notice if applicable

1.1.16

How can data subjects exercise their rights of access and to data portability?

How can data subjects exercise their rights to rectification and erasure?	
How can data subjects exercise their rights to restriction and to object?	
Existence of automated decision-making, including profiling?	
Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems.	
Automated decision-making is making a decision solely by automated means without any human involvement	
Profiling is the automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.	
You can only carry out this type of decision-making where the decision is:	
<ul style="list-style-type: none"> • necessary for the entry into or performance of a contract; or • authorised by domestic law applicable to the controller; or • based on the individual's explicit consent. 	
	Yes <input type="checkbox"/> No <input type="checkbox"/>
	If yes please provide details:
Will the solution use any form of Artificial intelligence (AI)?	

How much control will the data subjects have over the data being processed?	
1.1.17	

Would they expect you to use their data in this way?	
1.1.18	Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know <input type="checkbox"/>

Is Consent being relied upon for the processing of personal data?	
1.1.19	<input type="checkbox"/> Yes <input type="checkbox"/> No
How is the request for Consent managed? E.g. how consent is obtained, what is the data subject provided with, what is the process for the withdrawal of consent?	
1.1.20	
Where will the Consent be recorded?	
1.1.21	
Please provide the Patient Information Leaflet/Consent form	
1.1.22	

Purpose Limitation- Article 5(1)(b) of the GDPR says: “ Personal data shall be: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.”

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

Caldicott Principle 2 - Don't use personal confidential data unless absolutely necessary

Are there links to any wider initiatives or current projects?	
1.2.1	<p>Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>Please provide details:</p>

Data minimisation- Article 5(1)(c) of the GDPR says: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)”

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- Limited to what is necessary – you do not hold more than you need for that purpose.

Caldicott Principle 2: don't use personal confidential data unless absolutely necessary

Caldicott Principle 3: use the minimum necessary personal confidential data

What consideration has been taken to ensure that only the minimum data necessary is captured?	
1.3.1	
If the information is to be anonymised or pseudonymised in any way, specify how this will happen?	
1.3.2	

Accuracy- *Article 5(1)(d) of the GDPR says: Personal data shall be: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')*

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

Caldicott Principle 6: Understand and comply with the law

How will the accuracy (data quality) of the data be maintained?

1.4.1	
-------	--

Storage limitation- *Article 5(1)(e) of the GDPR says: Personal data shall be: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Caldicott Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Caldicott Principle 6: Understand and comply with the law

How long will the information be kept?

Please state the record type and associated retention period

[Retention Tool](#)

1.5.1	
-------	--

**How will the information be deleted/destroyed at the end of the retention period?
e.g. is this an automatic or manual process, please also include any SOP's**

1.5.2	
-------	--

Integrity and confidentiality (security)- Article 5(1(f) states You must ensure that you have appropriate security measures in place to protect the personal data you hold.

Caldicott Principle 4: access to personal confidential data should be on a need to know basis

Caldicott Principle 5: everyone with access to personal confidential data should be aware of their responsibilities.

Caldicott Principle 7: the duty to share information can be as important as the duty to protect patient confidential data

Who will have access to the data? Appropriate technical and organisational security measures:	
1.6.1	<div style="display: flex; justify-content: space-between;"> All UHNM Staff <input type="checkbox"/> Individual UHNM Staff member <input type="checkbox"/> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> Specific UHNM team/dept. <input type="checkbox"/> Third Party <input type="checkbox"/> </div> <p style="margin-top: 10px;">Please provide approximate numbers if accessed by team or third party and how access levels will be restricted: -</p>

Will the Trust require privileged accounts to be used?	
1.6.2	Yes <input type="checkbox"/> No <input type="checkbox"/>

Does the system support the use of Multi-Factor Authentication (MFA)?	
1.6.3	Yes <input type="checkbox"/> No <input type="checkbox"/>

If yes, please provide confirm which of the below authentication factor(s) are supported by the system.

	Strength	Authentication Factor	Factor Supported
1.6.4	Basic	SMS or voice message to trusted number	<input type="checkbox"/>
	Better	Mobile push notification	<input type="checkbox"/>
	Better	One-time password (OTP) generated by application or hardware token	<input type="checkbox"/>
	Better	Trusted end user device proved by a device certificate or similar	<input type="checkbox"/>
	Best	Public key infrastructure (PKI), such as NHS Care Identity Service smartcard	<input type="checkbox"/>
	Best	FIDO / WebAuthn or U2F	<input type="checkbox"/>

Please confirm which of the above authentication factors will be used by UHNM?
If MFA will not be used by UHNM please confirm why:

1.6.5	
-------	--

Security Arrangements	
------------------------------	--

1.6.6	
Please can you confirm that data within the system is encrypted to the NHS Standards at rest and in transit minimum of 256bit?	
Is there a security patching plan in place for the system, if so who is responsible for this and are critical patches applied within 14 days?	
Are role based access controls (RBAC) in place? <i>RBAC is where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions).</i>	
Please confirm where the information will be physically stored?	
Please describe the security controls protecting the location where the information is being stored?	
Please could you describe your local Business Continuity Plan?	

System Integration	
---------------------------	--

1.6.7	
Will the system be integrated with the Trust's Active Directory?	
Will the system be integrated with the Trust's PAS system?	
Will the system produce a clinical image/graphical output which should be retained? a) If yes all clinical images must be retained within the Trust's SECTRA PACS as part of the Trust's Digital Strategy. b) If integration with SECTRA PACS will not be possible please detail why.	

Supplier Details	
-------------------------	--

1.6.8	
Supplier:	

Product:	
Service Being Provided:	
Does the product/service involve the use of a 3 rd Cloud and if so does the supplier have a contract with the Cloud Supplier?	
Does the Supplier have Business Continuity Plans (attach evidence)?	
If information is to be shared, stored or accessed by a third party, please provide a description of the process including transfer and access authorisation methods.	

How will the data be accessed?	
1.6.9	Onsite <input type="checkbox"/> Off Site/Remotely <input type="checkbox"/>

State information transfer method:	
1.6.10	Email – nhs.net <input type="checkbox"/> Email – non nhs.net <input type="checkbox"/> Fax <input type="checkbox"/> E-fax <input type="checkbox"/> Telephone <input type="checkbox"/> Post <input type="checkbox"/> By hand <input type="checkbox"/> System feeds <input type="checkbox"/> Other –

National Data Opt Out:

For purposes other than the provision of direct healthcare, the Trust is required to consider a request to Opt-Out of any data sharing.

National data opt-out (should a patient request it) applies to the use of all confidential patient information for research and planning purposes.

The national data opt-out does not apply where:

- data is shared for direct patient care
- there is a risk to public health or data is required for monitoring and control of infectious diseases
- there is an overriding public interest; for example: reporting of gun wounds in line with GMC guidance

- there is a legal requirement to share information; for example: investigations by regulators of professionals (e.g. General Medical Council investigating a registered doctor’s fitness to practice)
- NHS fraud investigations
- notification of food poisoning
- consent obtained to take part in a specific project
- anonymised data is used
- data is used for local clinical audit
- data forms part of a national patient experience survey

When a national data opt-out needs to be applied, the entire record; or records, associated with that individual must be fully removed from the dataset used for this purpose.

National Data Opt-Out - Provide advice on how the project will meet this requirement:	
1.6.11	

Will the project require information to be transferred outside of the UK, or to receive information or be accessed from overseas?	
1.6.12	Yes <input type="checkbox"/> No <input type="checkbox"/> If yes please provide details:

If a Third party is involved, what arrangements are or need to be in place with the Trust, if known?	
---	--

1.7.1	Contract <input type="checkbox"/> SLA <input type="checkbox"/> Framework Agreement <input type="checkbox"/> Commissioned Service <input type="checkbox"/> Data Sharing Agreement <input type="checkbox"/> <input type="checkbox"/> Data Processing Agreement <input type="checkbox"/> NHS T&C’s <input type="checkbox"/> IDTA <input type="checkbox"/> NDA/Confidentiality Please provide details:
-------	--

If there is a contract in place, please confirm the Contract expiry date:	
--	--

1.7.2	Click here to enter a date.
-------	---

If known/applicable what information security procedures does the third party have in place?

1.7.3	<p>ICO registration Number <input type="checkbox"/> Reference:</p> <p>Data Security Protection Toolkit Compliance <input type="checkbox"/> Status:</p> <p>ODS Code:</p> <p>ISO Security 27001 <input type="checkbox"/> Cyber Essentials <input type="checkbox"/> Cyber Essentials Plus <input type="checkbox"/></p> <p>Please provide details (<i>embed Certification if available</i>):</p> <p>If the third party does not have the above security assurances, what other evidence can be provided e.g. Information Security policies. (embed evidence below)</p>
-------	--

Screenshot of the Data Security and Protection Toolkit status

1.7.3	Screenshot area
-------	-----------------

<u>DSP USE ONLY</u>		
Is there enough information to be assured that Principle 1 is met	YES	<input type="checkbox"/>
	NO	<input type="checkbox"/>

Section 2: Data Items

Personal Identifiable Data:																																	
2.2.1	<p>Personal details - Check all that apply:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> Forename</td> <td><input type="checkbox"/> Physical Description</td> <td><input type="checkbox"/> Location data e.g. IP address</td> </tr> <tr> <td><input type="checkbox"/> Surname</td> <td><input type="checkbox"/> Home Tel. Number</td> <td><input type="checkbox"/> Mobile Phone Number</td> </tr> <tr> <td><input type="checkbox"/> Address</td> <td><input type="checkbox"/> Other Contact number</td> <td><input type="checkbox"/> Legal Representative Name (Next of Kin)</td> </tr> <tr> <td><input type="checkbox"/> Post code (full)</td> <td><input type="checkbox"/> Email Address</td> <td><input type="checkbox"/> NHS number</td> </tr> <tr> <td><input type="checkbox"/> Post code (partial)</td> <td><input type="checkbox"/> GP Details</td> <td><input type="checkbox"/> Photographs/Images (PID)**</td> </tr> <tr> <td><input type="checkbox"/> Date of Birth</td> <td><input type="checkbox"/> Age</td> <td><input type="checkbox"/> Other</td> </tr> <tr> <td><input type="checkbox"/> Gender</td> <td><input type="checkbox"/> National Insurance No.</td> <td></td> </tr> </table> <p>Other – List any other data items or attach as an appendix</p> <p>Pseudonymised Information – Check all that apply:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> Unit Number</td> <td><input type="checkbox"/> Other ID number</td> </tr> </table> <p>Special Categories of Personal Data – Check all that apply:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> Racial or Ethnic Origin</td> <td><input type="checkbox"/> Political Opinion</td> <td><input type="checkbox"/> Religious Beliefs</td> </tr> <tr> <td><input type="checkbox"/> Trade Union Membership</td> <td><input type="checkbox"/> Physical or mental Health</td> <td><input type="checkbox"/> Sexual Life</td> </tr> <tr> <td><input type="checkbox"/> Sexual Orientation</td> <td><input type="checkbox"/> Genetic Data</td> <td><input type="checkbox"/> Biometric Data</td> </tr> </table> <p>Other – List any other data items or attach as an appendix</p>	<input type="checkbox"/> Forename	<input type="checkbox"/> Physical Description	<input type="checkbox"/> Location data e.g. IP address	<input type="checkbox"/> Surname	<input type="checkbox"/> Home Tel. Number	<input type="checkbox"/> Mobile Phone Number	<input type="checkbox"/> Address	<input type="checkbox"/> Other Contact number	<input type="checkbox"/> Legal Representative Name (Next of Kin)	<input type="checkbox"/> Post code (full)	<input type="checkbox"/> Email Address	<input type="checkbox"/> NHS number	<input type="checkbox"/> Post code (partial)	<input type="checkbox"/> GP Details	<input type="checkbox"/> Photographs/Images (PID)**	<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Age	<input type="checkbox"/> Other	<input type="checkbox"/> Gender	<input type="checkbox"/> National Insurance No.		<input type="checkbox"/> Unit Number	<input type="checkbox"/> Other ID number	<input type="checkbox"/> Racial or Ethnic Origin	<input type="checkbox"/> Political Opinion	<input type="checkbox"/> Religious Beliefs	<input type="checkbox"/> Trade Union Membership	<input type="checkbox"/> Physical or mental Health	<input type="checkbox"/> Sexual Life	<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> Genetic Data	<input type="checkbox"/> Biometric Data
<input type="checkbox"/> Forename	<input type="checkbox"/> Physical Description	<input type="checkbox"/> Location data e.g. IP address																															
<input type="checkbox"/> Surname	<input type="checkbox"/> Home Tel. Number	<input type="checkbox"/> Mobile Phone Number																															
<input type="checkbox"/> Address	<input type="checkbox"/> Other Contact number	<input type="checkbox"/> Legal Representative Name (Next of Kin)																															
<input type="checkbox"/> Post code (full)	<input type="checkbox"/> Email Address	<input type="checkbox"/> NHS number																															
<input type="checkbox"/> Post code (partial)	<input type="checkbox"/> GP Details	<input type="checkbox"/> Photographs/Images (PID)**																															
<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Age	<input type="checkbox"/> Other																															
<input type="checkbox"/> Gender	<input type="checkbox"/> National Insurance No.																																
<input type="checkbox"/> Unit Number	<input type="checkbox"/> Other ID number																																
<input type="checkbox"/> Racial or Ethnic Origin	<input type="checkbox"/> Political Opinion	<input type="checkbox"/> Religious Beliefs																															
<input type="checkbox"/> Trade Union Membership	<input type="checkbox"/> Physical or mental Health	<input type="checkbox"/> Sexual Life																															
<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> Genetic Data	<input type="checkbox"/> Biometric Data																															

Declaration	
2.2.2	<p>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</p> <p>If the Data is to be used for any other purpose then this DPIA will need to be reviewed or a 2nd DPIA will need to be completed, the DSP team will be able to advise</p> <p style="text-align: right;">Project Lead Confirms Understanding <input type="checkbox"/></p>

Section 3 – Data Flow - *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. If you are not clear on this yet, liaise with the DSP Team.*

Data Controller	Flow Description/ Identifier	Purpose	Direction	Recipient Status	Going from	Going to	Data type	Bulk Data 50+	Method of access/transfer	RPA Processing	Security protection controls	Where will the data be stored after access/transfer?	DPA Article 6(1)	DPA Article 9
			Choose an item.	Choose an item.			Choose an item.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.
			Choose an item.	Choose an item.			Choose an item.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.
			Choose an item.	Choose an item.			Choose an item.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.
			Choose an item.	Choose an item.			Choose an item.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.
			Choose an item.	Choose an item.			Choose an item.	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.	Choose an item.

Section 4 - GDPR

Description	Details
Identity of the Controller and Processor	
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of Personal Data	
Categories of Data Subject	
<p>Plan for return and destruction of the data once the processing is complete unless requirement under union or member state law to preserve that type of data.</p> <p><i>(Return/Destruction will apply to all applicable data and can and will take place throughout a contract period i.e. in line with legal retention periods for the relevant data type or when a particular dataflow is now longer required.)</i></p>	

Section 5 – Risk Assessment - Evaluate privacy/protection risks associated to the project (double click to edit)

<i>A unique coding that allows the risk to be easily identified</i>	or the initiative give rise to privacy risks? (Cause/ff)	potential or actual privacy risk(s) (Then)	potential Outcome (Resulting in)	Likelihood	Impact	RAG status	Assurances	approved/rejected by
1	If there is a server failure	Then...	Resulting in...					
2	If there is a software failure	Then...	Resulting in...					
3	If there is a network failure	Then...	Resulting in...					
4	If there is a loss of data	Then...	Resulting in...					
5	If the system is access by unauthorised individual	Then...	Resulting in...					
6	If staff are provided insufficient training of staff	Then...	Resulting in....					
7	If the system is lost or stolen	Then...	Resulting in...					
8	If there is a failure of the 3rd party to provide support	Then...	Resulting in...					
9	If the system could be used for fraud	Then...	Resulting in...					

Guidance on how to complete the risk assessment has been included below



Risk Assessment
 Guidance.docx

ACTION PLAN

DPIA Number	Ref	Date	Action	Individual Responsible	Action Due By	Status

Key

Complete / Business as Usual	Completed: Improvement / action delivered with sustainability assured.
On Track	Improvement on trajectory either: On track – not yet completed <i>or</i> On track – not yet started
Problematic	Delivery remains feasible, issues / risks require additional intervention to deliver the required improvement e.g. Milestones breached.
Delayed	Off track / trajectory – milestone / timescales breached. Recovery plan required.

Section 6 – DSP Review

Name	
Job Title	Data Security & Protection Manager
Signature	
Date	Click here to enter a date.
DSP Manager Advice/ comments	
Data Protection Officer Approval Sign off	
Name	Leah Carlisle
Signature	
Date	Click here to enter a date.
SIRO Approval Sign off	
Attach approval email	
Caldicott Approval Sign off	
Attach approval email	

Approved:	
Approved (with Conditions) <i>this is where the action plan and risk assessment would be reviewed</i>	
Rejected: <i>we can use our summary box to confirm why it was rejected</i>	

Appendices

Appendix 1: Risk Examples

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
- Non-compliance with sector specific legislation or standards
- Non-compliance with human rights legislation
- Non-compliance with the Data Protection Act or the General Data Protection Regulation

Appendix 2: Potential solutions

There are steps that can be taken to reduce a privacy risk; these are some examples of steps that could be taken to reduce a risk:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information
- Implementing appropriate technological security measures
- Ensuring that staff are properly trained and are aware of potential privacy risks
- Developing ways to safely anonymise the information when it is possible to do so
- Producing guidance for staff on how to use new systems and how to share data if appropriate
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.

- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.