DATA PROTECTION IMPACT ASSESSMENT

[Insert Project Title]

**IG Reference:** [To be added by Corporate IG]

**Status:** Choose an item.



**NHS England and NHS Improvement**

Enabling a lawful and ethical culture for the use of information

to deliver and improve our high-quality patient care

Data Protection Impact Assessment

Template version Control

|  |  |
| --- | --- |
| Template version | 7.1 |
| Published date | 29th March 2021 |
| Template owner | Corporate Information Governance |
| Classification | OFFICIAL |

1. Document contributors

**The Data Protection Impact Assessment (DPIA) is owned by the team undertaking the processing and will be completed with the support of data protection and records management specialists from the Corporate IG team.**

* 1. Document owners

**To be completed by the business lead.**

The individuals named below will be responsible for implementing all compliance activities required as a result of the assessment process.

**Business owner**

This should be the project or team lead responsible for completing this DPIA.

|  |  |
| --- | --- |
| Name |  |
| Job title |  |
| Team |  |
| Region or directorate |  |
| Telephone number |  |
| Email address |  |

**Senior Responsible Owner (SRO)**

This should be a relevant Band 9 or above accountable for the project or programme.

|  |  |
| --- | --- |
| Name |  |
| Job title |  |
| Telephone number |  |
| Email address |  |

* 1. Corporate IG specialist

**To be completed by Corporate IG.**

Corporate IG – the IG Officer, Manager or Lead supporting this DPIA.

|  |  |
| --- | --- |
| Name |  |
| Job title |  |
| Corporate IG work stream |  |
| Telephone number |  |
| Email address |  |

1. Data Protection Impact Assessment (Level 1)

To be completed by the business owner and emailed to Corporate IG.

* 1. Previous reviews

Has this project, programme or initiative been subject to a previous Data Protection Impact Assessment?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No/Unknown |  | If yes, provide IG reference of previous DPIA |  |

* 1. Purpose of the processing

Describe your project or initiative and the outcomes and benefits it hopes to achieve.

|  |
| --- |
|  |

What is the anticipated timeframe for your project or initiative?

|  |
| --- |
|  |

* 1. Description of personal data to be processed

Who will the data you intend to use be about (e.g. cancer patients, NHSE/I staff)?

|  |
| --- |
|  |

Please select all relevant options below to describe the data you will receive and use.

|  |  |  |  |
| --- | --- | --- | --- |
| Types of people |  | Number of people |  |
| Patients | Yes/No |  | Less than 100 | Yes/No |
| NHSE/I staff | Yes/No |  | Between 100 and 999 | Yes/No |
| Wider health and care staff  | Yes/No |  | Between 1,000 and 99,999 | Yes/No |
| Other  | Yes/No |  | Between 100,000 and 10m | Yes/No |
|  |  |  | Over 10m | Yes/No |
|  |
| Types of data |
| Data concerning health | Yes/No |
| Racial or ethnic origin | Yes/No |
| Political opinions | Yes/No |
| Religious or philosophical beliefs | Yes/No |
| Trade union membership information | Yes/No |
| Genetic data | Yes/No |
| Biometric data | Yes/No |
| Sex life or sexual orientation | Yes/No |
| Criminal convictions | Yes/No |
|  |  |
| Sensitivity of data |
| Contains identifiers (e.g. name, address, NHS number) | Yes/No |
| Data about individual people with identifiers removed | Yes/No |
| Summary or aggregated data that does not describe individual people | Yes/No |

* 1. How the personal data will be collected and used

Will all personal data to be processed for your project be received via the National Commissioning Data Repository (NCDR) or Strategic Information Platform (SIP)?

|  |
| --- |
| Yes/No |

If any personal data will be collected from sources other than the NCDR or SIP, describe where you will collect the personal data from.

|  |
| --- |
|  |

Describe how you intend to use this information and how you will ensure it is securely stored and managed.

|  |
| --- |
|  |

Will your use of the data result in automated decisions or actions being made about people in ways that could have a significant impact on them?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, how will this impact people |  |

Do you have a [Records and Information Management Co-ordinator (RIMC)](https://nhsengland.sharepoint.com/%3Ax%3A/r/sites/CIG/RM/_layouts/15/Doc.aspx?sourcedoc=%7B45B86215-A3B1-4578-B2CA-92A7CA5EE289%7D&file=RIMC%20Contact%20List.xlsx&action=default&mobileredirect=true&DefaultItemOpen=1&cid=d575b57b-134b-46e4-9ee8-66b872c3b40a) in your team?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, you should seek and record here their advice in relation to any [corporate records](https://nhsengland.sharepoint.com/sites/records1/Central/What%20is%20a%20record-42hyHKfw.pdf) this processing may generate |  |
|  |  |

If you do not have an RIMC, you may continue with the assessment. However, all teams should have a nominated co-ordinator, you must contact england.ig-corporate@nhs.net to arrange for a member of your team to be trained and registered.

Will NHS England and NHS Improvement colleagues be using a new IT platform that requires users to log in (i.e. with a username and password or other authentication process) or one that has substantially changed following a previous DPIA to process the personal data?

|  |
| --- |
| Yes/No |

If yes, you will need to produce or update a [System-Level Security Policy](https://nhsengland.sharepoint.com/%3Aw%3A/r/TeamCentre/TCO/infogov/_layouts/15/Doc.aspx?sourcedoc=%7B70D0A215-22AC-49D1-8BFA-F40277DF3FE0%7D&file=System%20level%20security%20template.docx&action=default&mobileredirect=true&cid=fde098bf-947c-4fa2-a40e-cc37ef6b5de4) (SLSP) before this review can be assured – please contact england.itsecurity@nhs.net. You must submit a copy of the approved SLSP with this DPIA to Corporate IG before your project can be signed off.

List any other organisations who will be given access to this data (for example, suppliers, data processors, contractors, consultancies, research agencies).

|  |  |  |
| --- | --- | --- |
| Organisation | Country of operation | Data to be shared |
|  |  |  |

* 1. Lawful basis for processing the personal data

What is it in statute or common law that enables and/or entitles NHSE, TDA or Monitor to use information about people in the proposed way? (For example, this might be a specific clause(s) within the NHS Act 2006 or the Health and Social Care Act 2012, a set of Regulations, Ministerial Directions, or a clear common law task. A list of NHS England and NHS Improvement’s statutory duties can be found [here](https://nhsengland.sharepoint.com/%3Aw%3A/r/sites/CIG/Shared%20Documents/Guidance/NHSEI%20Statutory%20Duties%20-%20January%202021.docx?d=w1120135a32294223abe19d29b473efe7&csf=1&web=1&e=O3ylbr).)

|  |
| --- |
|  |

Do any of the following statements apply?

|  |  |
| --- | --- |
| We need the information to enact a contract between us and the person to whom the data relates | Yes/No |
| We will be seeking explicit and unconditional consent from each person to which the data relates | Yes/No |
| We are responding to a legally binding request from a court or other statutory agency to provide this information | Yes/No |
| We need the information to protect the life of an immediately endangered individual or persons | Yes/No |

* 1. Risk assessment

This risk log should be updated throughout the DPIA process and may be contributed to by the business owner, IG Specialist, IG Management, the Data Protection Officer (DPO) or the SIRO.

Please record below any information risks associated with this programme, project or initiative. Several general information risks have been pre-populated and must be considered in all cases. Please also add any additional, project-specific information risks. All risks identified in this DPIA should be transferred to the project, programme or initiative’s local risk log for operational management by the business owner.

Risk scores should be calculated assuming any proposed mitigating actions have been successfully implemented, using the scoring matrix in the DPIA guidance.

| **Risk title** | **Description of how the risk impacts this activity or a justification of why it is not applicable** | **Risk score**(Prior to mitigations) | **Proposed solution(s) or mitigating action(s)** | **Action owner(s)** | **Action Due Date(s)** | **Risk score**(After mitigations are implemented) | **Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Impact | RAG status | Likelihood | Impact | RAG status |
| 1 | There is a risk that personal data may be misused by those with access |  | Select  | Select  |  Select |   |   |  | Select  | Select  |  Select | Select |
| 2 | There is a risk that insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls) |  | Select  | Select  |  Select |   |   |  | Select  | Select  |  Select | Select |
| 3 | There is a risk that insufficient technical measures are in place to ensure appropriate security of the personal data (e.g. encryption, access controls) |  | Select  | Select  |  Select |   |   |  | Select  | Select  |  Select | Select |
| 4 | There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures |  | Select  | Select  |  Select |   |   |  | Select  | Select  |  Select | Select |
| 5 | There is a risk that data that has had identifiers removed could be manipulated in some way to re-identify individual people |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |
| 6 | There is a risk that… |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |
| 7 | There is a risk that… |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |
| 8 | There is a risk that… |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |
| 9 | There is a risk that… |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |
| 10 | There is a risk that… |  | Select  | Select  |  Select |  |  |  | Select  | Select  |  Select | Select |

Thank you for completing the Level 1 Data Protection Impact Assessment. Please submit it to Corporate IG, where it will be assigned to a member of Corporate IG who will contact you to appraise the processing and complete the review. We aim to respond to you within ten working days.

1. DPIA (Level 1) Risk Screening

To be completed by the allocated Corporate IG specialist.

1. Type(s) of personal data

|  |  |
| --- | --- |
| Fully identifiable | Yes/No |
| Pseudonymised | Yes/No |
| Anonymised in context | Yes/No |
| Fully anonymised | Yes/No |

Will the processing involve fully identifiable data about patients?

|  |
| --- |
| Yes/No |

1. Risk thresholds

|  |  |  |
| --- | --- | --- |
| There is no processing of personal data involved in this activity | Yes/No | **If the answer to any of these statements is “Yes”, there is no need to progress further with the DPIA** |
| Data has been fully aggregated with small-number suppression applied prior to processing | Yes/No |
| NHS England and/or NHS Improvement is **not** a data controller or processor for this processing | Yes/No |

|  |  |  |
| --- | --- | --- |
| Any element of automated processing in which decisions are made about a person in the absence of human intervention (including profiling) | Yes/No | **If all these statements are answered “No”, progress as Level 1 DPIA**Complete Section 5 and seek local IG Manager approval**If the answer to any of these statements is “Yes”, progress as Level 2 DPIA**Complete Section 4 and Section 5 and seek DPO and SIRO approval |
| Processing of individual-level data that includes special categories or criminal convictions/offences (this does not apply to data from the SIP/NCDR or fully anonymised data) | Yes/No |
| Processing of fully anonymised data about more than 10,000,000 people that includes special categories or criminal convictions/offences | Yes/No |
| Systematic monitoring of a publicly accessible area involving more than 1,000 people | Yes/No |
| Transfer, storage or access of personal data outside of the UK | Yes/No |
| Any other risks to peoples’ rights and freedoms that cannot be mitigated below amber-red | Yes/No |

1. Data Protection Impact Assessment (Level 2)

To be completed by the business owner in discussion with the allocated IG Specialist if Corporate IG assess the processing as being high-risk.

* 1. Justification for personal data to be processed

Describe why it would not be possible to undertake your project or initiative without the personal data described in 2.3. Explain why this is the minimum amount of data necessary for the task and, if applicable, why you could not use de-identified data.

|  |
| --- |
|  |

Is the provision of personal data obligatory?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, describe why this is the case |  |

What are the possible consequences for a data subject if there is a failure to provide the requested personal data?

|  |
| --- |
|  |

If the processing will result in a decision being made about an individual without any human intervention, describe the logic by which any decisions will be reached?

|  |
| --- |
|  |

Will any personal data be used for direct marketing to data subjects?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, provide further details |  |

* 1. Additional information about personal data to be processed

Describe the dataset(s) that you intend to collect and process, who will have access to it and how it will be securely stored. Please either submit a comprehensive data flow diagram or complete the section below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Dataset** | **Personal data items** | **To be accessed by** | **Secure storage** |
|  |  |  |  |

List any flows of personal data into NHS England and NHS Improvement.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sender** | **Content** | **Secure transfer mechanism** | **Recipient** |
|  |  |  |  |

List any flows of personal data out of NHS England and NHS Improvement.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sender** | **Content** | **Secure transfer mechanism** | **Recipient** |
|  |  |  |  |

Will the personal data be recoverable in the event of a physical or technical incident?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, explain how or refer to SLSP |  |

If you are using a data processor, are arrangements in place to securely return or destroy the personal data at the end of the contract?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, explain how or refer to SLSP |  |

Will it be possible to provide an individual, or another organisation, a copy of their personal data in a structured, commonly used and machine-readable format? Note this only applies in limited circumstances – your IG Specialist will support you with this.

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No/NA |  | If yes, explain how |  |

* 1. Correspondence with data subjects

Approval of this DPIA will require you to comply with NHS England and NHS Improvement’s Subject Rights Requests and Incident Management procedures, which are administered by Corporate IG.

Will you be able to retrieve the personal data relating to an individual if they request it?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, explain how or refer to SLSP |  |

Explain how you will monitor the quality and maintain the accuracy of the personal data, including its rectification or erasure, where necessary.

|  |
| --- |
|  |

* 1. Consultation

Describe how you have sought, or intend to seek, the views of data subjects who will be subject to the processing. If you do not intend to consult with data subjects, explain why this is the case.

|  |
| --- |
|  |

Describe how you have sought, or intend to seek, advice from relevant stakeholders (e.g. clinicians, security experts, research governance, ethicists, Corporate ICT, NHS Digital, Public Health England) where their specialist knowledge would be useful in understanding and managing privacy risks.

|  |
| --- |
|  |

1. IG Assessment

To be completed by a Corporate IG specialist in discussion with the business owner and records management colleagues.

* 1. Controllers, processors and third parties

Confirm the controller(s) for this processing.

|  |  |  |
| --- | --- | --- |
| NHS England | Yes/No |  |
| Trust Development Authority | Yes/No |
| Monitor | Yes/No |

List additional joint controller(s) for this processing and upload evidence of the compliant joint data controller arrangements (e.g. Joint Controller Agreement).

|  |  |
| --- | --- |
| Organisation | Evidence of arrangements |
|  |  |

List data processors associated with this processing and upload evidence of the relevant data protection clauses (e.g. Data Processing Agreement) and completed assurance checklists.

|  |  |  |
| --- | --- | --- |
| Organisation | Agreement | Checklist |
|  |  |  |

List other controllers with whom personal data will be shared as part of the processing and associated Data Sharing Agreements.

|  |  |
| --- | --- |
| Organisation | Data sharing agreement |
|  |  |

List any Commissioning Support Units or Hosted Bodies that will undertake processing of personal data for this purpose and provide a copy of the relevant SLA or MoU that commissions the work.

|  |  |
| --- | --- |
| CSU | MoU or SLA |
|  |  |

* 1. International Transfers

If any of the organisations listed in Section 2.4 will process personal data outside of the UK, describe the arrangements in place. Ensure copies of any contractual agreements (e.g. standard contractual clauses, binding corporate rules) are attached in Section 5.1 above.

|  |  |  |
| --- | --- | --- |
| Organisation | Location | Control |
|  |  | Choose an item. |

* 1. Lawful basis

Confirm the GDPR Article 6 condition for the processing.

|  |  |
| --- | --- |
| Art 6.1a Consent | Yes/No |
| If yes, explain how consent will be sought and how data subjects can revoke it if required |  |

|  |  |
| --- | --- |
| Art 6.1b Contract | Yes/No |
| If yes, describe the contract between NHSE/I and the data subject |  |

|  |  |
| --- | --- |
| Art 6.1c Legal obligation | Yes/No |
| If yes, describe the legal obligation to which NHSE/I needs to adhere |  |

|  |  |
| --- | --- |
| Art 6.1d Vital interests | Yes/No |
| If yes, describe why processing the data is necessary to protect someone’s vital interests |  |

|  |  |
| --- | --- |
| Art 6.1e Public authority | Yes/No |
| If yes, detail the clause(s) from an Act or Regulation that describes the legal duty |  |

|  |  |
| --- | --- |
| Art 6.1f Legitimate interests | Yes/No |
| If yes, describe NHSE/I’s legitimate interests to process this data |  |

Will the processing involve special categories of personal data?

|  |
| --- |
| Yes/No |

If yes, confirm the GDPR Article 9 condition for the processing.

|  |  |
| --- | --- |
| Art.9.2a Explicit consent | Yes/No |
| Art.9.2b Employment, social security, social protection law | Yes/No |
| Art.9.2c Vital interests | Yes/No |
| Art.9.2d Political, philosophical, religious or trade union not-for-profit body  | Yes/No |
| Art.9.2e Data manifestly made public by the data subject | Yes/No |
| Art.9.2f Legal claims | Yes/No |
| Art.9.2g Public interest  | Yes/No |
| Art.9.2h Health or social care system  | Yes/No |
| Art.9.2i Public health | Yes/No |
| Art.9.2j Archiving, scientific or historical research | Yes/No |

Will the processing involve disclosing data that is subject to a duty of confidentiality for a purpose other than direct care?

|  |
| --- |
| Yes/No |

If yes, confirm the lawful basis for processing.

|  |  |
| --- | --- |
| Consent | Yes/No |
| Safeguarding | Yes/No |
| Covered by Section 251 decision | Yes/No |
| Required by law (e.g. COPI regulations) | Yes/No |
| Overriding public interest | Yes/No |

* 1. Information asset management

Does an information asset already exist in relation to this processing?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, provide the asset number |  |
|  |  | If no, confirm the new IAO  |  |
|  |  | If no, confirm the new IAA(s) |  |

* 1. Records and information management

Will [corporate records](https://nhsengland.sharepoint.com/sites/records1/Central/What%20is%20a%20record-42hyHKfw.pdf) be created or managed as part of this processing?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, identify the types of record |  |
|  |  | If yes, confirm where the records will be stored |  |
|  |  | If yes, provide the retention period for the personal data and the basis for this retention period (e.g. [corporate retention schedule](https://nhsengland.sharepoint.com/sites/thehub/Policy%20library/Forms/AllItems.aspx?id=%2Fsites%2Fthehub%2FPolicy%20library%2FCorporate%20records%20retention%20schedule%2Epdf&parent=%2Fsites%2Fthehub%2FPolicy%20library), applicable guidance or rationale) |  |
|  |  | If yes and where records are processed outside of NHSE/I premises or systems, how will they be securely returned for the remainder of the retention period(s) as and when this becomes necessary (e.g. following the closure of the project)? |  |
|  |  | If yes, name of Corporate Records Management specialist who has reviewed the processing |  |

* 1. Fair processing

Is NHS England and NHS Improvement exempt from providing fair processing information under provisions specified in the UK GDPR?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, describe exemption | Choose an item. |

If no, is the processing sufficiently described in NHS England and NHS Improvement’s [central privacy notice](https://www.england.nhs.uk/contact-us/privacy-notice/how-we-use-your-information/)?

|  |
| --- |
| Yes/No/Update Required |

If no or update required, complete the template below.

|  |  |
| --- | --- |
| Purposes for processing |  |
| Sources of the data |  |
| Categories of personal data |  |
| Recipients of personal data |  |
| Legal basis for processing |  |

Is personal data collected directly from data subjects?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, confirm that local privacy information exists and complies with [this guidance](https://nhsengland.sharepoint.com/%3Aw%3A/r/sites/CIG/Shared%20Documents/Guidance/Local%20Privacy%20Information%20Guidance%20v1.3%20%28June%202018%29.docx?d=wcc31419ab0df4f4ba5c5964fbfe2cbf5&csf=1&web=1&e=SrLLxg)  | Yes/No |
|  |  |

* 1. Reviewers

|  |  |
| --- | --- |
| Caldicott Guardian (only required for Level 2 DPIAs) | Yes/No |
| If confidential, identifiable patient information will be processed, summarise Caldicott Guardian’s advice here. |  |
| Name of Caldicott Guardian |  |
| Date advice provided |  |

|  |  |
| --- | --- |
| Information Commissioners’ Office (only required if requested by DPO/SIRO) | Yes/No |
| If the DPO or SIRO request that the ICO review the processing, summarise their advice here. |  |
| Name of ICO contact |  |
| Date advice provided |  |

1. Approval

All Level 1 and Level 2 DPIAs must be assessed and assured by a Corporate IG Manager, Senior Manager or SMT Lead via section 6.1.

Processing activities subject to a Level 2 DPIA must also be submitted to the national Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO) for approval – complete section 6.2.

* 1. Actions required

Select all mandatory actions that apply to this processing from the list below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Applies** | **Due date or pre-go-live** | **Complete** |
| RIMC trained | Yes/No/NA |  | Yes/No/NA |
| Asset registered or updated on IAMS | Yes/No |  | Yes/No/NA |
| Local privacy information provided | Yes/No/NA |  | Yes/No/NA |
| Data processing and sharing agreements signed | Yes/No/NA |  | Yes/No/NA |
| Data processor assurance checklists reviewed | Yes/No/NA |  | Yes/No/NA |
| SLSP developed and reviewed by Info. Sec | Yes/No/NA |  | Yes/No/NA |
| Mitigation of outstanding risks | Yes/No/NA |  | Yes/No/NA |

List any additional actions specific to this project or initiative below.

|  |  |  |
| --- | --- | --- |
| **Action** | **Due date** | **Status** |
|  |  | Yes/No |

* 1. DPIA Assurance (Level 1 and Level 2)

|  |  |
| --- | --- |
| Outcome of IG Management assurance | Choose an item. |
| Date of IG Management assurance |  |

Corporate IG Manager, Senior Manager or SMT Lead

|  |  |
| --- | --- |
| Name |  |
| Job title |  |
| Corporate IG work stream |  |
| Telephone number |  |
| Email address |  |

Submit Level 2 DPIAs to england.dpo@nhs.net for consideration by the Data Protection Officer and Senior Information Risk Owner

* 1. DPIA Approval (Level 2 only)

|  |  |
| --- | --- |
| Outcome of SIRO assessment | Choose an item. |
| Date of SIRO assessment |  |

Does the Data Protection Officer have any concerns regarding this processing that they feel have not been sufficiently mitigated?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes/No |  | If yes, provide details |  |

Data Protection Officer or deputy

|  |  |
| --- | --- |
| Name |  |
| Job title |  |
| Email address |  |

Senior Information Risk Owner or deputy

|  |  |
| --- | --- |
| Name |  |
| Signature |  |
| Job title |  |
| Email address |  |

Ensure that this DPIA and its status is logged on the IG Advice Register and a copy saved in the relevant SharePoint folder.