

Data Analytics Platform

Data Protection Impact Assessment

February 2025

v3.1



**NHS fraud.
Spot it. Report it.
Together we stop it.**

Executive Summary

The document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: **'OFFICIAL-SENSITIVE'**

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Table of contents

Executive Summary	2
Links & Dependencies	6
1. Data Protection Impact Assessment Requirement & Process	7
Introduction.....	7
Data Analytics Platform - General Description	8
Data Protection Impact Assessment.....	8
Ownership	31
Section 1: Data Maintenance and Protection Overview.....	31
Section 2: Uses of the Application and the Data.....	31
Section 3: Data Retention.....	33
Section 4: Internal Sharing and Disclosure of Data	33
Section 5: External Sharing and Disclosure of Data	33
Section 6: Notice/Signage	33
Section 7: Rights of Individuals to Access, Redress and Correct Data.....	34
Section 8: Technical Access and Security.....	34
Section 9: Technology	35
DPA 2018 Compliance Check	36
The Privacy and Electronic Communications Regulations.....	36
The Human Rights Act.....	36
The Freedom of Information Act	36
Conclusion.....	36
Annex A - Definition of Protected Personal Data	37
Annex B - Data Protection Compliance Check Sheet	38

OFFICIAL

Document Control					
PM	Ref	Document owner	Version No	Issue Date	Amendments
	DPIA – SAS Analytics Platform	DPO	V0.1	April 2022	Initial creation
	DPIA – SAS Analytics Platform	DPO	V0.2	April 2022	Redraft and update
	DPIA – SAS Analytics Platform	DPO	V1.0	June 2022	Finalised draft following comments from IA
	DPIA – SAS Analytics Platform	DPO	V1.1	June 2022	Updated following review by Information Governance
	DPIA – SAS Analytics Platform	DPO	V1.1	July 2022	Finalised with confirmation from SMT lead for mitigation
	DPIA – SAS Analytics Platform	DPO	1.2	July 2022	Updated following Data Strategy Group
	DPIA – Data Analytics Platform	DPO	1.3	April 2023	Updated following software changes (ensuring remains relevant)
	DPIA – Data Analytics Platform	DPO	2.0	Dec 2024	Updated to give current position and incorporate Project Athena considerations
		DPO	3.1	Feb 2025	Finalised draft following review by IG Lead

Prefix	
Reference:	DPIA Data Analytica Platform
Date:	10th December 2024
Author:	Data Acquisition Manager
Data Owner:	N/A (dependant on the data being processed)
Version:	3.1
Supersedes	3.0

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	May 2018	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.
2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.
3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.
4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:
 - a. "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data¹..."
5. Under GDPR you must carry out a DPIA where for example you plan to:
 - a. process special category or criminal offence data on a large scale.
6. The ICO also requires a DPIA to be undertaken for example, where you plan to:
 - a. use new technologies;
 - b. match data or combine datasets from different sources;
 - c. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

¹ GDPR - Recital 75

8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.
9. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Data Analytics Platform - General Description

10. This document contains information in relation to the NHSCFA data analytics platform and the associated processes and practices. This is designed to extend to any software package that is utilised by NHSCFA for data processing, analysis and dissemination purposes, particularly given the possibility of both replacements and additions to this software. Within scope of this DPIA is focus will primarily be on the storage, processes, analysis and outputs as opposed to individual pieces of software itself. Additionally, although this DPIA will reference key datasets, it is only in the context of this analytical platform and instead defers to individual DPIA's undertaken for each example of utilised datasets. Should any changes occur that apply to any issues of privacy, this DPIA will be updated (see 12)
11. As a number of individual assessments exist for the numerous NHSCFA data sources themselves, this DPIA is completed to consider the system itself and the manner that it may process data generally in the above manner. As such it does not concern itself with individual sources of data as these particulars are covered under more specific DPIAs
1. This is the third iteration of the DPIA concerning the data analytics platform and has been carried out primarily to incorporate changes in activity as a result of Project Athena, as well as the addition of new key datasets and technologies. It has been undertaken by the Data Acquisition Lead, in consultation with the Information Governance Officer and Information Governance and Risk Management Lead, with wider support of the Analytical intelligence Team, and Project Athena functions within NHSCFA, acting as a means to service the needs of both consecutively.
12. The Data Analytics Platform, in addition to GDPR, is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

13. To ensure the databases and systems meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template² comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

² Version 0.3 (20180209)

Step 7 - Sign off and record outcomes

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The purpose of the Data Analytics Platform can be split into the following activities:

- Transforming and preparing data prior to building, configuring, administering, and deploying customisable dynamic web-based reports. These enable users to access their own data without the need for enhanced IT or analytical skills as many of these functions and calculations are prepared by the Analytical Intelligence Unit prior to release.
- Producing management information reports for strategic and tactical purposes to enable operational and management decision making to take place from an informed position.
- Querying, exploring and analysing data to support the strategic work within the NHS business plan and to answer parliamentary questions (PQs), Freedom of Information requests (FOIs) and other unplanned requests for information (RFIs) made by Ministerial, HMG, NHS, internal and external stakeholders. Examples of this include statistics for the Annual Report, Corporate and organisational dashboards.
- Exploring, analysing and profiling current and historical data to identify statistical trends, patterns and anomalies not identifiable through normal methods of examination used to proactively identify fraud and where needed the ability to amend predefined parameters as well as code. In additions, tools and unsupervised learning techniques are used where the problem relevant data is suitable to do so.
- Transformation including matching, merging, filtering, extraction, analysis, profiling and mining of data for intelligence assessments and individual fraud investigations producing meaningful summaries as well as granular pattern level extraction output using large datasets.
- Designing, developing, transforming, testing, deployment, maintenance and access control of NHSCFA databases.
- Deployment, configuration, maintenance, troubleshooting and access control (both internal and external) for the Business Intelligence software enabling analysis to be undertaken and appropriate dissemination of information and intelligence.
- Importing, transforming, storing, maintaining, securing and updating datasets dynamically and making them available for analysis.
- Building, configuring and deploying secure web based dynamic reports for external NHS users.
- Building and distributing reports with Row Level Permissions to both internal and external stakeholders to ensure appropriate but limited access to individual tables and the data contained therein.

--

In 2024 NHSCFA commenced Project Athena, a pilot project aiming to both prevent fraud and deliver a dedicated response by identifying patterns in data on a scale that has never been done before across the NHS for counter fraud purposes. For the purposes of this DPIA, the considerations associated with Project Athena are included alongside the "business as usual" elements and the assessments and mitigations within this DPIA are to be considered as universal and equally relevant to both.

Because the nature of the full extent of the data analytics platform as a wide array of software and tools that can be utilised in accordance with the above, as well as the wide-ranging nature of data types that can be processed, it has been considered necessary to consider the above activities as applied within a single data platform and review them collectively within the DPIA framework as a single entity for review.

Additionally, because of the unique and specific considerations concerning individual datasets and their basis for access and use, there is a need to relegate some specific risks and mitigations to be considered separately, as part of the DPIA process for the data sources themselves.

Additionally, the following considerations may apply, as cited in Part 1:

- a) There is the possibility from some data sources that personal data may be processed by the platform
- b) The tool utilises new technologies
- c) The intention match data or combine datasets from different sources.
- d) The intention to collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?
2. What is the source of the data?
3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?
4. Why types of processing identified as 'likely high risk' are involved?

1. How will you collect, use, store and delete data?**Collection:**

Data utilised by the analytics platform will be collected from data sources either within NHSCFA or from external data sources. In the case of external data sources, NHSCFA would coordinate the particulars of this extract with the data owner directly to organise and manage the request, stemming from the requirements through to the data share itself. In either circumstance, a NHSCFA Data Engineer / Database Specialist or Information Analyst/ Information Specialist would import the data onto the platform and create a view or dataset for analysts to commence exploration and transformation.

Utilisation:

How the data will be used would be project specific, however generally speaking the outcomes would be either

- a) Information Analysts will undertake analysis to determine outliers using a range of appropriate measures, this could range from rule-based analysis or data matching to the development of machine learning models and algorithms, as dictated by the problem centric approach and insight that needs to be derived.
- b) The creation of formal records that determine the activity and outcome, usually in the form of some type of written report that describes the extent of the fraud risk, the methodology applied and the insight that has been possible from the activities above. This will necessarily utilise the data to demonstrate these points and highlight the appropriate considerations and reflects necessary (this may be through aggregation of datasets, or utilization of specific pieces of data to demonstrate outliers, provide examples and determine salient points for consideration)
- c) Depending on the findings themselves, the basis for sharing and processing the data and the strength of the outliers, as well as the Information Sharing agreements and any wider DPIA:s for individual datasets, it is possible that the outliers may be shared with either the external data providers or NHSCFA's own investigative services for further action.
- d) Information Analysts produce a data-based output, for example an electronic dashboard or statistical physical report detailing output and findings, that is utilised to support NHSCFA activity and, where necessary, is shared with the wider NHSCFA, wider NHS or any external stakeholder (examples range from responses to an Freedom of Information enquiry, provision of benchmarking data provided to support counter fraud activity to wider NHS organisations or a physical report focused on a specific problem and detailing the analysing and findings found in relation to identified fraud risks).
- e) Where there is a need to formalise the outputs drawn from the findings, submission of a Technical Appendix document, which may include specific references to the data, will be submitted to the Data Strategy Group to allow oversight and approval of the outcomes.

Storage:

The storage of the data is on the NHSCFA secure cloud, following migration in January 2022 to a cloud based solution hosted on Microsoft Azure.

Additionally, the introduction of Microsoft Fabric, in support of Project Athena, provides wider mechanisms for storage within the NHSCFA through its use as an end-to-end analytics and data platform that encompasses data movement, processing, ingestion, transformation, real-time event routing and report building.

Retention:

Retention is managed via the following formal documents which are maintained by NHSCFA:

- Data Retention Schedule
- Information Asset Register
- Inventory of Information Transferred (IIoT)

Through these, datasets are mapped in terms of their content, origin and, schedules are set for deletion and removal. NHSCFA also proactively review their data and will remove records once there is no longer a clear and specific purpose for their continued use (in line with the requirements of the relevant legislation and guidelines that apply).

2. What is the source of the data?

The sources of the data would be project and purpose driven and this covers a wide range of data sources, too numerous to name. However, there are a number of key data systems and data owners that are internal and external to the NHSCFA and would be considered fundamental to expected / business as usual activities for the software. These may include:

Internal:

- NHSCFA Case Management System (CLUE), as well as legacy systems (FIRST)
- NHSCFA Intelligence Database (IBase)
- Performance Reporting Database (Verto) as well as legacy systems (MRT)
- The LCFS/DoF nominations database (CPOD)

External

- The NHS provider and commissioning sectors via the NHSCFA Data Capture System (DCS) as calibrated for specific data capture exercises
- NHS staff and the general public via the NHSCFA Fraud and Corruption Reporting Tool (FCROL) –n.b This data is gathered indirectly, through records captured via CLUE and Ibase
- NHSBSA Dental services data (project specific)
- NHSBSA Pharmaceutical routine data source e.g. monthly payment schedules (project specific)
- HM Cabinet Office via National Fraud Initiative (NFI) data (project specific)
- External open-source data (e.g. Companies House, Ordnance Survey etc)
- The Secondary Use Service (“SUS”), a dataset concerning secondary care, made available through the NHS England Unified Data Analytics Layer (UDAL)

This list is not intended to be extensive and instead to reflect the breadth and diversity of NHSCFA data sources. Individual sources are instead identified within the documents cited above and additionally through identification and recognition of their characteristics in individual DPIA's.

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

The purpose and application of data that is processed by the Data Analytics Platform is project driven and may include the following:

- Sharing findings (outliers) internally for the purposes of intelligence, loss measurement and investigation and/or to support fraud prevention activity to mitigate identified fraud risks
- Sharing findings externally with the data controllers to support their own remedial activity and fraud prevention
- Provision of summary data internally and externally to support a variety of performance reporting techniques that measure the impact of activity within NHSCFA and across the wider NHS

4. Why types of processing identified as 'likely high risk' are involved?

Although it is impossible to be specific as each type of data processed will pertain to the requirements and defined objectives of the project that warrant it, there is some potential for the use of high-risk data. However, the nature of NHS fraud concerns deceptive and dishonest activity concerning the treatment of patients and the services and support activity that support the NHS in delivering this function. The data that identifies this fraud therefore necessarily pertains to these activities and, in doing so, may contain information about associated persons, for example alleged perpetrators and witnesses – which may include NHS patients and the members of staff.

In particular, outlier detection that relates to the treatment of patients may necessitate details of individual steps of clinical activity provided to individual patients in order to determine courses of linked treatment.

Finally, the case management system contains information about ongoing and concluded investigations and some fields, particularly those which are free text, may be utilised. Because there is no assurance that these free-text fields do not contain personal data, these must also be included.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?
2. How much data will you be collecting and using?
3. How often?
4. How long will you keep it?
5. How many individuals are affected?
6. What geographical area does it cover?

1. What is the nature of the data and does it include special category or criminal offence data?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

2. How much data will you be collecting and using?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

3. How often?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

4. How long will you keep it?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these. As described above, NHSCFA maintains a register of data assets which is used to consider and schedule retention of data and these would be applied to the appropriate data source

5. How many individuals are affected?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

6. What geographical area does it cover?

Although these would be specific to each project, as a general rule the NHSCFA only provide services to the NHS in England and it would be expected that any access and use of external data sets within the NHSCFA data platform would solely relate to English data. However, NHSCFA are contractually commissioned to provide some services for the Welsh Government, which may include reporting of Welsh data within NHSCFA internal datasets (for example the Case Management System), however these do not extend to fraud detection using data.

In each case this would be a fact that will be confirmed in the specific DPIA for their use.

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?
2. How much control will they have?
3. Would they expect you to use their data in this way
4. Do they include children or other vulnerable groups?
5. Are there any prior concerns over this type of processing or security flaws?
6. Is it novel in any way?
7. What is the current state to technology in this area?
8. Are there any current issues of public concern that you should factor in?
9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

1. What is the nature of your relationship with the individuals?

Although these would predominantly be specific to each project and the data sources being applied, the category of individual can be summarised in the following manner:

- Patients and other types of service user
- NHS Employees (including clinicians as well as other support workers and administrative staff)
- Person(s) otherwise concerned with NHS fraud cases

However, in terms of the specifics, this would defer to the DPIA and other data usage considerations being applied for each project or data source.

2. How much control will they have?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

3. Would they expect you to use their data in this way

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

4. Do they include children or other vulnerable groups?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

5. Are there any prior concerns over this type of processing or security flaws?

Although these would predominantly be specific to each project and the data sources being applied, the nature of NHS fraud and the data that exists in relation to it (in any context) it would be expected that this would have potential to be contentious as it is likely to concern the treatment of patients and may

require information about the recipient of treatments or NHS employees who provided or supported this work

6. Is it novel in any way?

This would be dependent on each project and the data sources being used and techniques being applied.

7. What is the current state to technology in this area?

The NHSFCA data platform makes use of a range of tools and their use and role will be specific to the project and therefore are best summarised in the corresponding DPIA for that dataset. However for the purposes of outlying the current operating model, the following technologies apply:

Alteryx is a cloud based analytical system that utilises the Alteryx software package for data processing, It was procured on 31st March 2021 for a 3 year licence following a tender exercise, fitting the specifications of the organisation. The tool is accompanied by use of PowerQuery and PowerBI for external reporting transformation, report creation and dissemination of data. Key elements of the tools used include:

- Extract, Transform and Load (ETL): Pulling data from one source, transforming the data into a standardised format and placing it into another database.
- Analytics / Data Mining: Querying both structured and unstructured data to provide information to internal and external stakeholders, analysing data to identify trends and create rules-based processes to highlight anomalies as well as utilising data mining techniques both supervised and unsupervised to pro-actively identify anomalies or fraud patterns of criminality which are indicative of fraud.
- Reporting & Distribution of Information software: Providing secure static and dynamic management reports for all units within the business and to our external stakeholders via a web portal platform.

Following its purchase in November 2024, NHSCFA are also utilising Microsoft Fabric as the next generation software for use in NHSCFA's data science framework. Fabric is an all-in-one data analytics solution that covers everything from data movement to data science, real-time analytics, and business intelligence. It offers a wide range of data products available to users, which fall under the four buckets: Data ingestion, data storage, data engineering and data science and business intelligence.

These tools serve a similar function to the tools that NHSCFA are using currently, including those summarised above, but collectively the tool provides a range of benefits and efficiencies, in particular the "one lake", which eradicates data silos and the need to create multiple copies of a dataset. Additionally, all (tabular) data in One Lake is stored in one format, called "Delta Parquet" which is an open file format. This solves the data integration problem and data storage sizing as it's a compressed file format and allows. Data scientists, data engineers, data analysts to work with the same data, in the same format. Finally, Fabric provides a unified user experience and one access control method & one security model. This ensures access control and security is simplified and effective, with one access control method and one security model, applied across all tooling and experiences. Access to resources is principally managed through Workspaces, which are a collection of Fabric items, and because all data is within One Lake, data governance and discoverability become a much easier task through data lineage option. Fabric comes with a single built-in Monitoring Hub, which monitors all Fabric activity and thus supports enhanced security for all elements within the data science process.

8. Are there any current issues of public concern that you should factor in?

NHS fraud is, in itself, a matter of public concern and the use of data to combat it, particularly when this might concern information about patients and other service users, whilst ensuring that it is applied in an appropriate and proportional matter, are all issues of public concern.

These concerns also extend to the protection of data from loss or theft and controls and oversight to ensure this does not occur.

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

NHSCFA codes of conduct are summarised in the following documents:

Information Governance:

- Information Governance Policy
- Information breach Reporting Policy
- Data Quality Policy
- GDPR – Data Protection Policy

Information Security:

- Information Security Policy
- NHSCFA Acceptable use Policy

The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network.

Describe the purposes of the processing:

1. What do you intend to achieve?
2. What is the intended effect on individuals?
3. What are the benefits of the processing, for you and more broadly?

1. What do you intend to achieve?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for the data and the specific use case(s) associated

However, in line with the .NHSCFA strategy, in all instances the activity will align with the NHS Strategic pillars, tackling fraud and economic crime against the NHS by using the data platform to:

1. **Understand:** Understand how fraud, bribery, and corruption affect the NHS.
2. **Prevent:** Ensure the NHS takes proactive action to prevent future losses.
3. **Respond:** Respond effectively to detected fraud.
4. **Assure:** Demonstrate continuous improvement in prevention, detection, and recovery.

2. What is the intended effect on individuals?

These would be specific to each project and the data sources being applied and therefore would defer to the DPIA and other data usage considerations being applied for these.

3. What are the benefits of the processing, for you and more broadly?

The benefits of any processing would be specific to each project. However briefly summarised they would be directly or indirectly in support of fraud detection activity within the NHS and in support of the NHSCFA organisation in meeting these aims.

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

STEP 3: Consultation process

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

This would be specific to each project and the data sources being applied within it, as each would be subject to their own considerations concerning and the nature of the data, who it pertains to, where it is sourced from and how it is being applied.

Generally speaking, informing stakeholders via the NHSCFA website or individual engagement opportunities or exercises therefore would defer to the individual project and the DPIA and other data usage considerations being applied for these will consider these options.

2. Who else do you need to involve within your organisation?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

3. Do you need to ask your processors to assist?

There are no identified circumstances where non NHSCFA processors would directly assist in the handling and processing of data being utilised by NHSCFA's data platform - the extent of external parties involvement would be limited to indirect support, for example in terms of insight generation and domain expertise concerning the data and its usage.

In all cases, this activity would be specific to the project and the data sources being applied within it, as each would be subject to their own considerations concerning and the nature of the data, who it pertains to, where it is sourced from and how it is being applied in conjunction with the high-end aims of that particular piece of work. Therefore this would be a key part of the initial considerations when commencing this course of work and subject to the DPIA that is produced in terms of those considerations. Assessment, Therefore, this would primarily be specific to each project and the data sources being applied and the nature of the data and who acts as the data controller and would be outlined in the corresponding DPIA.

4. Do you plan to consult information security experts or any other experts?

See Q3 above, this would be specific to each project and the data sources being applied and the nature of the data and who it pertains to. This support all of the technological considerations outlined in NHSCFA has a wealth of expertise in this domain within its organisation and it is unlikely to need any direct consultation

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?
2. Does the processing actually achieve your purpose?
3. Is there another way to achieve the same outcome?
4. How will you prevent function creep?
5. How will you ensure data quality and data minimisation?
6. What information will you give individuals?
7. How will you help to support their rights?
8. What measures do you take to ensure processors comply?
9. How do you safeguard any international transfers?

1. What is your lawful basis for processing?

This would primarily be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

However, generally speaking The NHSCFA's remit of preventing, detecting and investigating fraud, corruption and unlawful activities against or affecting the Health Service in England is defined in the 2017 [Secretary of State Directions](#), which concerns the establishment of the NHSCFA alongside the directions to NHS organisations, including arms length bodies, that concern cooperation and provision of data (section 3)

This is underpinned by the following legislation:

Basis for accessing personal data

The basis for processing any personal data within the platform is supported by Articles 6 and Article 10 of the Data Protection Act 2018, specifically:

6(1) This condition is met if the processing—

(a) is necessary for a purpose listed in sub-paragraph (2), and

(b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

(a) the exercise of a function conferred on a person by an enactment or rule of law;

(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

10(1) This condition is met if the processing—

(a) is necessary for the purposes of the prevention or detection of an unlawful act,

(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and

(c) is necessary for reasons of substantial public interest.

(2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3) In this paragraph—

- *“act” includes a failure to act;*
- *“competent authority” has the same meaning as in Part 3 of this Act (see section 30).*

The specific UK GDPR articles this relies on are as follows:

Article 6:

(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;

Article 9:

(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;

(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.

Basis for processing Sensitive Data

NHSCFA data concerns NHS activity, which necessarily links to a variety of treatment and wider clinical services. These, alongside other sensitive forms of personal data, may also be processed and in this instance the following elements of the Data Protection Act 2018 (DPA) Schedule 8, sections 1 and 8 applies as follows:

1 This condition is met if the processing —

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

8(1) This condition is met if the processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and

(b) consists of—

(i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,

(ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or

(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, “anti-fraud organisation” has the same meaning as in section 68 of the Serious Crime Act 2007.

2. Does the processing actually achieve your purpose?

Broadly speaking, this is resoundingly the case, however the circumstances that this is achieved would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

3. Is there another way to achieve the same outcome?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

4. How will you prevent function creep?

Although this would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied, the parameters of each data application would be linked to the objectives of each data source and/or application and this would be outlined in the appropriate documentation – whether it be linked. The NHSCFA has a range of oversight tools, ranging from Project Boards to the centralised Data Strategy Group, and supporting governance and assurance processes, which can manage and mitigate this risk (this is also reflected in key roles within the organisation in terms of SRO’s etc).

5. How will you ensure data quality and data minimisation?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

6. What information will you give individuals?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied. More broadly speaking, section 5b of Schedule 15 of GDPR negates the need to directly inform data subjects where a) the provision of such information proves impossible or would involve a disproportionate effort, or b) such notification may to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available.

Accordingly, NHSCFA maintain a range of pages online that outlines our use of personal data and provides an in-depth mechanism for informing patients, service users and any stakeholders about the activity NHSCFA provides, the basis under which it acts and the standards NHSCFA holds itself to in terms of managing records. NHSCFA also have a mechanism for answering queries or concerns which is advertised on these pages.

7. How will you help to support their rights?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied.

8. What measures do you take to ensure processors comply?

This would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied, however engagement and collaboration for stakeholders is a key element of the vast majority of NHSCFA work – as the centralised body for counter fraud activity, our activity is continually conjoined with additional stakeholders and this would include the provision of MoUs and ISA's that are very clear about the expectations for compliance and cooperative activity in terms of data provision and what is/isn't permitted.

9. How do you safeguard any international transfers?

Although this would be specific to each project and the data sources being applied and the nature of the data and who it pertains to and how it is being applied, it would be expected that the transfer of data across international borders is extremely unlikely given the mandate of NHSCFA and the service it provides exclusively to England and Wales.

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	Likelihood of harm Remote, Possible or Probable	Severity of harm Minimal, Significant, or Severe	Overall risk Low, Medium or High
1. There is a risk that personal data will be used for purposes other than that which are stipulated in the business case	Possible	Significant	Medium
2. There is a risk that complex processing of data by participating authorities during the analysis process may lead to information being inadvertently disclosed.	Remote	Significant	Medium
3. There is a risk that data disclosed are not required for the purposes of fraud detection, or are excessive.	Remote	Minimal	Low
4. There is a risk that incorrect information may be disclosed by participating authorities during the pilot.	Possible	Significant	Medium
5. There is a risk that data is retained for longer than it is needed	Possible	Minimal	Low
6. There is a risk that an individual's rights under GDPR are violated.	Remote	Significant	Medium
7. There is a risk that an external attacker gains access to personal data.	Remote	Significant	Medium

OFFICIAL

<p>8. There is a risk that information could be lost, released or shared inappropriately</p>	<p>Remote</p>	<p>Significant</p>	<p>Medium</p>
<p>9. There is a risk that processing is carried out internationally in a territory without appropriate personal data protection in place</p>	<p>Remote</p>	<p>Minimal</p>	<p>Low</p>
<p>10. There is a risk that individuals will be misidentified as a result of data processing</p>	<p>Possible</p>	<p>Significant</p>	<p>Medium</p>
<p>11. There is a risk that the quality of data will not be to a consistently high standard</p>	<p>Possible</p>	<p>Significant</p>	<p>Medium</p>

STEP 6: Identify measures to reduce risk

<p>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.</p>	<p>Effect on risk</p> <p>Eliminated, Reduced, Accepted</p>	<p>Residual risk</p> <p>Low, Medium, High</p>	<p>Measure approved by SMT Owner</p> <p>Yes/No</p>
<p>(1) There is a risk that sensitive data will be used for purposes other than that which are stipulated in the business case</p>	<p>(1), (2), (3) Robust governance structure and project management techniques are used to make clear roles and responsibilities,</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(2) There is a risk that complex processing of data by participating authorities may lead to information being inadvertently disclosed.</p>	<p>(1), (2), (3) Robust governance structure and project management techniques are used to make clear roles and responsibilities, timelines, data flows, and contingency plans. The data itself has been minimised to remove personal data from the structured data, ensure that all possible steps have been taken to prevent inclusion of personal data (beyond that included in unstructured data)</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(3) There is a risk that incorrect information may be disclosed by participating authorities during the pilot (leading to incorrect identification of fraud)</p>	<p>(1), (2), (3) Robust governance structure and project management techniques are used to make clear roles and responsibilities, timelines, data flows, and contingency plans. The data itself has been minimised to remove personal data from the structured data, ensure that all possible steps have been taken to prevent inclusion of personal data (beyond that included in unstructured data)</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(4) There is a risk that incorrect information may be disclosed to unauthorised parties</p>	<p>(4) Data quality review is undertaken by authorities sharing data to review individuals / organisations included and remove irrelevant ones from the matching process.</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(5) There is a risk that data is retained for longer than it is needed</p>	<p>Each data source is subject to a range of mapping and corresponding retention schedule which is completed manually and overseen by human input</p>	<p>Low</p>	<p>Yes - TM</p>

OFFICIAL

<p>(6) There is a risk that individual's rights under GDPR are violated</p>	<p>(6) This risk is not considered to be increased beyond business-as-usual levels as a result of the considerations in this DPIA and those in corresponding DPIA's for individual datasets</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(7) There is a risk that an external attacker gains access to personal data</p>	<p>(7) NHS CFA have approved and assured methods of managing data and for information security and are ISO27000 compliant. The data analytical platform itself is password protected and secured on the Cloud.</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(8) There is a risk that information could be lost, released or shared inappropriately</p>	<p>(8) This risk can be mitigated with robust governance structures, as well as security accreditation and adherence to a common set of data standards, set out in the security statement and information sharing agreement.</p>	<p>Low</p>	<p>Yes - TM</p>
<p>(10) There is a risk that individuals could be misidentified as a result of data processing.</p>	<p>(10) Any decisions made using matched data will be informed by the strength of the match and resulting outlier. The strength of all outputs from the</p>	<p>Low</p>	<p>Yes - TM</p>

<p>(11) There is a risk that the quality of data will not be to a consistently high standard</p>	<p>Data Platform will be assessed to manage false positives and triage follow up investigations.</p> <p>(11) Data quality reviews are routinely undertaken as part of the analytical process and the impact of these findings will impact on the outputs produced. In terms of outlier detection, low data quality can sometimes be a useful factor in determining fraud risks.</p>	<p>Low</p>	<p>Yes - TM</p>
--	---	------------	-----------------

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:	5 th July 2022	Confirmed approval to authorise
Residual risks Approved by SMT Owner:	5 th July 2022	Confirmed approval to authorise
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
<p>Summary of DPO advice:</p> <p>Having reviewed the DPIA I am satisfied that a comprehensive assessment of the NHSCFA Data Analytics platform has been undertaken. Primary access to the platform will be by approximately 30 members of staff which includes database administrators and data engineers, with permission role-based access and therefore will be fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.</p>		
DPO advice accepted or overruled by:	17 th February 2025	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by the Information and Records Management Officer:		The DPO should also review ongoing compliance with DPIA

Ownership

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	
Data Protection Officer	

3. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the NHSCFA Data Analytics Platform was assessed as OFFICIAL.
2. The following measures briefly describe what controls have been implemented to protect the Data Analytics Platform and the personal data recorded:
 - a. The NHSCFA Data Analytics Platform is primarily accessed by approximately 30 members of staff from NHSCFA, which includes the database administrators and Data Engineers. However, outputs and wider data disseminations are specific to individual projects and their designated outcomes.
 - b. The Data Analytics Platform has direct interconnections with other NHSCFA systems and applications, particularly in terms of data drawn in from other NHSCFA data sources. Each of these have their own access control measures and controls in place to mitigate any risk of unauthorised access. The nature of each would be specific to each project and their intended data usage
 - c. The Data Custodian must comply with the data protection requirements. Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
3. It is assessed that there are no residual privacy risks to the personal data used by the Data Analytics Platform, which cannot be addressed through the management and oversight related to individual projects
4. This DPIA must be reviewed to note any changes in the NHSCFA operating model or if any changes are made to the manner that it concerns use of personal information or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

5. Administration of the Data Analytics Platform is managed by the Database Administrators and Data Engineers, currently within the Technology Team and roles specific to Project Athena. Requests for

OFFICIAL

changes / amendments to the system are managed by the NHSCFA Service Desk who are the first point of contact and record and manage requests.

6. Information in the Data Analytics Platform would be project and purpose driven - this covers a wide range of data sources too numerous to name. However, there are a number of key data systems and data owners that are internal and external to the NHCFA and would be considered fundamental to expected / business as usual activities for the software. These are

Internal:

- NHSCFA Case Management System (CLUE), as well as legacy systems (FIRST)
- NHSCFA Intelligence Database (IBase)
- Performance Reporting Database (Verto) as well as legacy systems (MRT)
- The LCFS/DoF nominations database (CPOD)

External

- The NHS provider and commissioning sectors via the NHSCFA Data Capture System (DCS) as calibrated for specific data capture exercises
- NHS staff and the general public via the NHSCFA Fraud and Corruption Reporting Tool (FCROL) –n.b This data is gathered indirectly, through records captured via CLUE and Ibase
- NHSBSA Dental services data (project specific)
- NHSBSA Pharmaceutical routine data source e.g. monthly payment schedules (project specific)
- HM Cabinet Office via National Fraud Initiative (NFI) data (project specific)
- External open-source data (e.g. Companies House, Ordnance Survey etc)
- The Secondary Use Service (“SUS”), a dataset concerning secondary care, made available through the NHS England Unified Data Analytics Layer (UDAL)

7. Some of the above data sources capture sensitive data. The individual DPIA's for each would be more specific in outlining what these are. It is not necessarily the case that the information captured on these systems will be transferred or otherwise processed by the Data Analytics Platform, although this may be the case for individual datasets, which must be recorded appropriately in the corresponding DPIA>

8. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

9. The Data Analytics Platform is subject to NHSCFA Data Handling and Storage Policy by virtue as to how this is applied to the individual data sources that it processes. All records are electronic and there are no paper based records produced by this system.

10. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

11. Because of the nature of the Data Analytics Platform in producing and disseminating data, the Database/System is theoretically accessible by all members of staff from NHSCFA, however this is not to say that all the applications of outputs will be utilised in this widespread manner and more targeted controls (and alternative mediums) are available to produce and disseminate data that requires restricted audiences. Access of the main system is restricted to nominated member of staff within NHSCFA, including the supporting functions necessary for configuration and use of these tools, for example those concerned with data engineering, database administration etc.

Section 5: External Sharing and Disclosure of Data

12. The only information shared directly with external organisations would be a) through controlled sharing of findings via formal reports and b) via the dissemination element of the analytical platform which would be designed specifically to produce reports for external users.

Ultimately, individual projects which MAY have this element would require their own considerations, as would the data sources that capture these data in the first place. The nature of this dissemination is specific to each project, and it is extremely unlikely any would include personal data. However, the disclosure of data via electronic reporting can be controlled through rigorous security settings, linked to the NHSCFA nomination process and database.

Individual outliers would be shared in specific circumstances, if necessary for the administration of justice and/or in accordance with appropriate Information Sharing Agreement/Memorandum of Understanding.

Section 6: Notice/Signage

13. NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

Section 5b of Schedule 15 of GDPR negates the need to directly inform data subjects where a) the provision of such information proves impossible or would involve a disproportionate effort, or b) such notification may to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available

NHSCFA maintain a range of pages online that outlines our use of personal data and provides an in-depth mechanism for informing patients, service users and any stakeholders about the activity NHSCFA provides, the basis under which it acts and the standards NHSCFA holds itself to in terms of managing records. NHSCFA also have a mechanism for answering queries or concerns which is advertised on these pages.

14. The use of signage or other notifications to notify the public of the gathering and use of personal data for wider systems is not relevant to this Data Platform and therefore outside the scope of this DPIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

Right to Access

15. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

18. It is unlikely that many access requests will be received as the personal data recorded is all in relation to individual data sources and/or their outputs, as opposed to the platform itself which acts as intermediary.

19. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

20. All NHS employees and members of the public have the right to request access, redress and correct personal data recorded about them, however this may need to be considered in light of the below

Right for deletion

21. Were NHSBSA to be subject to a request for deletion by a data subject who wishes their data deleted from that processed by NHSCFA for the purposes outlined, we note that 3b of Article 17 of the UK GDPR “the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller” would apply and be sufficient to deny this request.

22. The basis for this refusal concern A) the prevention and detection of fraud within the NHS overwhelmingly supports the public interests and B) the defined function of NHSCFA as an official authority, supported the NHSCFA Establishment Order and the Secretary of State for Health Directions. This is in line with guidance from the ICO which identifies the appropriateness of the above.

Right to object

23. Given that none of this data concerns direct marketing, the absolute right to object is not relevant. Nonetheless individuals have the right to object to the processing of their personal data at any time, even where a task is carried out in the public interest, in line with official authority and/or legitimate interest.

24. Again, the ICO have provided guidance on the Right to object | ICO which confirms that the applicant must give specific reasons why they are objecting. NHSCFA/NHSBSA would need to determine if they have compelling legitimate grounds which override the interests of the use in detecting/preventing fraud. If an individual cites that processing is causing them substantial damage or distress (e.g. the processing is causing them financial loss), the grounds for their objection will have more weight. This, however, is very unlikely.

25. It would be necessary to document the considerations and outcomes and may also be possible to give assurance through the extent that NHSBSA/NHSCFA already partly comply with this request through use of the masking techniques (see question 17).

26. The answers above provide a generic response, which may not encapsulate wider reasons that NHSBSA has to consider requests of this nature, associated with their own basis for processing. In the interests of ensuring that specific considerations were made for individual circumstances

Section 8: Technical Access and Security

27. The security and technical access architecture of the Database/System is as explained in this DPIA. The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to the ISO27000 and ISO27001

28. Access to the system itself, with the exception of disseminated products, is restricted to internal staff only.

29. The technical controls to protect the database include:

- a. Anti-virus protection;
- b. Permission based access controls to shared drive.
- c. Logging, audit and monitoring controls.
- d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

30. The Database/System holds personal information obtained electronically and is located in the NHS Counter Fraud Authority cloud infrastructure, subject to the principles of use outlined in the following NHSCFA policies

- Information Governance Policy
- Information breach Reporting Policy
- Data Quality Policy
- GDPR – Data Protection Policy
- Information Security Policy
- NHSCFA Acceptable use Policy

DPA 2018 Compliance Check

1. The DPO must ensure that the System, and the personal data that it records, and its business activities, are compliant and maintain compliance with:
 - a. The GDPR and the Data Protection Act in general;
 - b. The Data Protection Principles;
 - c. The interpretations of the Principles.
2. **This is not a recommendation but a requirement of law.**
3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.
4. The Database/System processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed (see Annex B) describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with.

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

8. There are no residual privacy risks to the personal data recorded in the Data Analytics Platform that are not inherent to the individual projects or data sources that make use of them, however this DPIA provides a further basis to consider the elements inherent to the platform itself and these have been reflected and recorded appropriately, and thus will dovetail with wider DPIA's that concern individual datasets and their application. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	Information Analytics
Project	Data Analytics Platform

2. Contact position and/or name, telephone number and e-mail address.

(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	
Branch / Division	
Phone Number	
E-Mail	

3. Description of the programme / system / technology / legislation (initiative) being assessed.

(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

The purpose of the system is for collecting, collating, managing, analysing and disseminating information in support of all internal business units and externally to the NHS and DH. It is also used to manage the data and the analysis tools used to identify patterns and anomalies that may indicate fraudulent behaviour.

The resulting analyses can be used in a number of project specific ways. Detected outliers may be used to support on-going investigations as well as support the creation of intelligence that can prompt new investigations. The findings can also drive changes to policy and guidelines in order to address fraud risks. Data can additionally be used to provide electronic Management-style information reports, in some cases linking to other data sources or being adapted to new formats (i.e. graphical representation via graphs or adapted to show weighting or ratios for benchmarking purposes)

Because the scope for the types of data that the system can process is universal, and the wide-ranging nature of data types that can be processed by it for individual projects and data exercises (which may include personal data), it has been determined that a specific DPIA should be produced to cover this processing specifically, as a separate review to the original datasets and/or projects that this activity supports

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to protect NHS staff from economic crime and the Data Analytics Platform facilitate this work through the provision of data services. This can take a variety of shapes and purposes (as described above), which in turn is defined by the project itself and its objectives. The system itself is universal in acting as the conduit for the data source(s) that need to be utilised – this can include any data source owned or accessed by the NHSCFA for their counter fraud purposes .

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of the potential for any personal data that might be gathered and utilised by the system. In most cases, specific DPIA considerations relate to the data source itself and/or the project utilising it. However, this DPIA considers specifically the role of the Data Analytics Platform in applying it.

As such, the data in the Data Analytics Platform is been gathered for a specific, justifiable and proportional purpose (as outlined by the data source and/or the data project) and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is a revision of existing DPIA's carried out on the system, previous iterations of which are summarised in the Document Control section of this document...

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

**IMPORTANT NOTE:*

'Personal data' means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And 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.

See main document that this checklist appends.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

7th Floor,
10 South Colonnade (10 SC),
Canary Wharf, London, E14 4P

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH