NHS Counter Fraud Authority

S12 Local Exercise
Data Protection Impact Assessment

May 2025

V1.0

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

Executive Summary

This document contains information in relation to the S12 Local Exercise, which is the name given to an exercise being undertaken in collaboration between NHSCFA and a range of NHS organisations, concerning a rolling programme of work that concerns a proactive data exercise to detect outliers that can be indicative of fraud.

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'**

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

Table of contents

Prefix	
Reference:	**DPIA – S12 Local Exercise**
Date:	**12th May 2025**
Data Owner:	**NHSCFA / originating NHS organisations**
Version:	**1.0**
Supersedes	**N/A**

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 data[1]…"

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.
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**.

[1] GDPR - Recital 75

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.

S12 Local Exercise - General Description

10. This DPIA concerns a proposed joint exercise (henceforth "the exercise") between NHSCFA and a range of NHS organisations henceforth "the participating NHS organisations") who participate in a collaborative exercise over a rolling period. The exercise concerns fraud risks identified within the claims process for Section 12 mental health referrals, which as part of the treatment during Mental Health Act assessments (MHAA) involves several steps to ensure that doctors are properly compensated for their work. More specifically, the exercise, regarding sharing and access of the claims data to identify fraudulent practice. This DPIA is produced alongside a range of Information Sharing Agreement (ISA) produced between NHSCFA and the organisations, with a view to supporting the process for data sharing with an assessment of the personal data considerations associated with the project.

11. The data this DPIA concerns is, in most cases, drawn from the S12 Solutions Platform ("S12"). S12 is a digital tool used by NHS organisations to organise Section 12 Mental Health Act (MHA) processes. it supports organising Mental Health Assessments and the clinicians undertaking them. The primary use of the tool concerns the ability to connect Approved Mental Health Professionals (AMHPs) with Section 12 doctors. The platform helps AMHPs find available Section 12 doctors to support mental health services and also facilitates the creation and submission of Electronic Claim Forms which users and approvers can create, sign, and share electronic statutory MHA forms. Where organisations do not use the S12 software tool, the standardised nature of the Claims Form also allows inclusion of wider submissions for this purpose.

12. The relevance of the data, whether drawn from the S12 platform and the data within it, or from separate claims forms, concerns a recognised and substantiated fraud risk regarding false claims This includes, but is not limited to, duplicate claims, claims which were not carried out and other forms of disruptive activity. This type of activity has been identified through reactive work undertaken by NHSCFA and this exercise is intended to be a proof-of-concept that widens the scope of this work through a proactive exercise with additional organisations, designed to identify deviant patterns of behaviour on a larger scale.

13. This is the first DPIA to be completed and it has been carried out by the Data Acquisition Manager, in consultation with the Senior Proactive Counter Fraud Response Officer responsible for leading the exercise, alongside the support and oversight of the Information Governance and Risk Management Lead.

14. The exercise, 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

15. To ensure the exercise 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 template[2] comprised of seven steps:

Step 1 - Identify the need for a DPIA

[2] Version 0.3 (20180209)

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

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 primary outcome of this exercise is concerned with a data share between the organisations to support the detection of outliers that may be indicative of fraud. This will be achieved through a complex data science led approach, produced in conjunction with domain experts, it would determine a framework that would determine outliers likely to be fraudulent. The findings, and the methodology, would then be subjected to assurance methodologies within NHSCFA that would scrutinise it as being appropriate for categorisation as a “fraud detected” figure through the strength of the analytics and rule-based approach in determining these outliers The specific data this concerns has been identified as part of an drafted Information Sharing Agreement which acknowledged that this proposed data share would necessarily concern personally identifiable data (although not special categories of personal data) and limited recourse for anonymisation/pseudonymisation whilst still achieving the aims of the exercise. . The Parties are subject to the duty of confidentiality owed to those who provide them with confidential information and the confidentiality and security of this information in line with the statutory and other constraints on the exchange of information are recognised, including the requirements of the UK GDPR, the Data Protection Act 2018, the Freedom of Information Act 2000 and the Human Rights Act 1998. As such, it was deemed necessary to produce a DPIA to record the recognised risks, considerations and mitigations that apply and ensure that, alongside the ISA itself, a transparent and auditable record of this exercise was produced

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?

The data will be collected by NHSCFA from participating NHS organisations via extractions from the S12 Software and/or collation of the MH claims form using local systems. In each case this data will be made available via an Excel spreadsheet, which will be password protected and shared between the participating NHS organisation and NHSCFA via nominated individuals.

Upon receipt, data will be stored on the NHSCFA secure environment, specifically Microsoft Fabric and analysis undertaken using DataBricks.

The data used as part of a proactive counter fraud exercise, the primary outcome of which concerns the detection of outliers that may be indicative of fraud. Through a complex data science led approach, Analysts will utilize data to undertake analysis to determine anomalies in the claims data in order to determine and identify outliers which could be indicative of fraud. The outcomes of which would be summarised in a data-based output, for example an electronic dashboard or statistical physical report detailing output and findings, that is utilised to support a summary of the NHSCFA activity and outputs which may contain sample, aggregated or summarized excerpts of the data.

The findings, and the methodology, would then be subjected to assurance methodologies by NHSCFA and the participating NHS organisations that would scrutinise and validate them, and deem as being a) appropriate for further outcome within a "business as usual" approach that aligns with the counter fraud remit of both organisations and b) values associated with the claims as appropriate for categorisation as a "fraud detected" figure through the strength of the analytics and rule-based approach in determining these outliers

In line with the ISA, Information shall be stored in accordance with the individual Parties' records retention and disposal schedule and unless stated otherwise (or in the absence of a records retention and disposal schedule, or a statutory retention period) the information shall not be retained for longer than is necessary to fulfil the specified purpose of the exercise. Data will be deleted using an approved method by an NHSCFA Data Engineer, with specific records made concerning the deletion and notification of the relevant parties (e.g. the originating trust and any wider data controllers) that this has occurred,

2. What is the source of the data?

The source of the data is a range of participating NHS organisations, who will opt in to participate over the course of the exercise via individual data sharing arrangements and corresponding documentation.

The data source will be data drawn from the Claims forms used to record payments for Section 12 mental health assessments. These will predominantly come from the S12 Solutions platform; a digital tool used by the participating NHS organisations to organise and streamline Mental Health Act (MHA) processes in England and organise efficiencies in organizing Mental Health Assessments and the clinicians undertaking them.

The primary use of the tool concerns the ability to connect Approved Mental Health Professionals (AMHPs) with Section 12 doctors. The platform helps AMHPs find local, available Section 12 doctors to support mental health services and also facilitates the creation and submission of Electronic Claim Forms which users and approvers can create, sign, and share electronic statutory MHA forms.

However, because the Claims form is universal in terms of content and format, it is possible for submission of claims data to be collated and provided without the use of the S12 software, thus allowing participation from NHS organisations who do not use this software, but capture the data in a consistent manner.

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

The underlying principle of this exercise concerns a series of data shares between individual NHS organisations and the NHSCFA and the reciprocation of results and supporting domain expertise. This DPIA is produced in conjunction with an Information Sharing Agreement which support and formalises this approach.

In line with the Information Sharing Agreement produced with each participating organisations, which includes the agreed sharing of findings, intelligence and case management info etc no wider third parties will be recipients of the data itself as part of this exercise, however in circumstances where any individual outlier can be utilised for further action than the information would be diverted to a 'business as usual' process for national or local investigation which would undertake its own specific data share, as needed and these may be shared with wider parties (particularly in the event of any criminal or civil action that necessities disclosure).

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

This exercise necessarily undertakes certain types of processing that are identified as "likely high risk", for example, large scale data processing, matching or combining datasets and the innovative use of new technology. This is the necessary evolution of the wider work that has prompted the exercises as the risk concerning S12 data and the associated false claims. These have been identified through reactive work undertaken by NHSCFA and this exercise is intended to be a proof-of-concept that widens the scope of this work through a proactive exercise with additional organisations, designed to identify deviant patterns of behaviour on a larger scale and thus allow wider and more extensive management of the issue.

The choice of processing is deliberate and other types of high-risk processing – such as automated decision making, evaluation of scoring, use of sensitive data - have deliberately been avoided in order to mitigate any risk and/or prevent any inappropriate use or outcomes from this exercise.

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?

The full extent of the data requirements is within Appendix A, however to summarise:

- The specific data this concerns is that drawn from S12 claims, which are either drawn from the S12 Solutions platform or individual S12 claims forms. The claims form pertains to reimbursement of Section 12 Mental Health Assessments, and the clinicians requesting and undertaking them and their claims for financial reimbursement for providing this service

- It is also necessary to determine the approval process of the S12 claims, which will include the approver/authoriser of the claim, as this will identify collusion and inappropriate dissemination of S12 cases and/or self-certification of claims

- It is additionally necessary to have a patient identifier within the data, to identify and distinguish duplication of claims from dual attendance. For this purpose the patient initials will be utilised. In the absence of any wider data, this is not sufficient for identification by the NHSCFA (directly or indirectly) and thus the data can be considered anonymised from a patient perspective.

The actual data concerned is identified in Appendix A and although this includes personally identifiable data, it does NOT contain any special category or criminal offence data. The personal data is explicit and the use of it is unavoidable, given the need of this exercise for the purposes of data matching from a range of sources (particularly where pseudonymisation of the clinicians and approvals is not possible, due to the range of originating data sources) and the need to ensure distinction to allow matching. Similarly, a patient identifier is required to determine cases of duplicate records from multiple-attendances and thus is used to ensure distinctiveness and prevent false positives.

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

As a result of the nature of this exercise, it is not possible to quantify how much data will be utilised. Each data share will be organised with individual organisations over a rolling period over the length of this exercise and the extent will be agreed in terms of appropriateness with the participating organisation. As the intention is to undertake an extract of the desired data from the S12 system or corresponding Claims Form from each of the participating organisations, the extent of which will depend on the availability of consistent data and the time period they cover.

Due to the “opt in” nature of the exercise, the number is participating NHS organisations will increase over a rolling period. However, the number of Section 12(2) approved doctors and Approved Clinicians in England is relatively low, given the qualifications required for the role.

Where the exercise is able to produce a basis for fraud disruption activity. it will be necessary to undertake remeasures (see below) to determine fraud prevention activity, however the amount of data necessary will depend on the speed of implemented disruption.

3. How often?

In the first instance, it will be necessary to undertake an initial data share from each participating NHS organisation. Dependent on the scale and extent of the findings, and the ability for the NSHCFA Response Team and the participating NHS organisation, to undertake additional detection and prevention, it is envisaged that there may be opportunities to undertake a subsequent data share in order to measure the impact of such activity. This may result in numerous iterations of the data over several periods, dependent on the scale and extent of the findings and the ability to garner counter fraud impact from conjoined activity, as influenced by the findings.

4. How long will you keep it?

The information shall not be retained for longer than is necessary to fulfil the specified purpose or purposes and it is estimated that the exercise can be undertaken and concluded over 2025/26 (at which point, at the end of Q4 of 25/26, NHSCFA will undertake a review of this exercise and all others association with Project Athena).

5. How many individuals are affected?

Because it is not possible to identify the number of organisations who will participate over the course of this project, it is not to quantify how many individuals will be affected by the exercise. Only a small sample of NHS mental health staff are qualified to undertake Section 12 Mental Health services – estimated to be less than 5000 in England – and naturally not all of these will be in participating organisations

6. What geographical area does it cover?

The scope of the exercise is determined by the area covered by the service provisions of the participating organisations only. This has yet to be determined in terms of participation but will be limited to mental health services across England.

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 they 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?

The category of individuals can be summarised as Mental health specialists providing services on behalf of the NHS, within the context of the Mental health services provided by each of the participating NHS services. As such, these have no direct relationship with NHSCFA.

2. How much control will they have?

Data subjects will have no control, as this would not be appropriate given that the purpose of this exercise is for counter fraud detection. In this instance, Rights for Deletion and Rights to Prevent Processing are not applicable (see below) and the NHS England Opt Out process is also not pertinent. Each of these elements has individual considerations, outlined later in this DPIA, but the overarching sentiment in each case this is related to the performance of tasks in public interest and the detection and prevention of crime (fraud).

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

One would expect claims submitted for NHS payment would be scrutinised and that proactive fraud detection methods would also be undertaken to prevent false claims and other forms of dishonest behaviour, particularly in response to identified threats of dishonest practice.

Additionally, there are notifications within the S12 software, as well as wider privacy notices, that identify that data will be subject for scrutiny for counter fraud purposes, although the extent they are utilised will be individual to each participating organisation

It is less likely that it would be expected that this activity would need to be facilitated via a data share and so, as part of the opt-in process and information sharing protocols within each organisation, recommendations will be made to consider the current and potential notification of staff (this, in turn, will act as a form of disruption) to the extent that, as Data Controller, they are satisfied that their responsibilities are met

4. Do they include children or other vulnerable groups?

No.

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

No

6. Is it novel in any way?

This exercise is partially novel, in that it builds on previous data shares and activity undertaken by NHSCFA. However, it widens the scope and scale of detection to complement the existing work and add a new area of advanced analytics which can derive new findings. These can then be utilised in the fight against fraud - and the particular form of fraud being examined is one that has been identified as a specific risk that has taken place and so this will further substantiate these concerns.

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

The originating 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 this toolset itself. However for the purposes of outlining the current operating model, the following applies

a) Microsoft Fabric

Following its purchase in November 2024, NHSCFA are 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.

Alongside a range of optimisation and efficiencies, Microsoft Fabric offers several governance features to help manage, protect, and monitor NHSCFA data and provide sufficient governance, this includes:

- An admin portal to control the overall Fabric estate, including tenant, domain, and workspace settings and group and individual permissions
- Data security features like data loss prevention, information protection, and metadata scanning to secure sensitive information
- Data Discovery and Trust: Tools to encourage data discovery, trust, and reuse, such as endorsement and data lineage
- Business continuity and disaster recovery tools to prevent data loss and corruption
- Monitoring and insights capabilities to monitor data access and usage and to uncover insights, and act on them, ensuring continuous improvement and compliance.

Fabric meets several UK-relevant compliance standards to ensure data security and privacy, including:

1. **ISO/IEC 27001**: Information security management
2. **ISO/IEC 27017**: Cloud-specific security controls
3. **ISO/IEC 27018**: Protection of personal data in the cloud
4. **ISO/IEC 27701**: Privacy information management

The full list can be found here

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.

b) Databricks

NHSCFA has implemented Databricks in Q4 of 2024/25, designed to work alongside Fabric for the actual analytical tool. Databricks is a powerful solution for data analysis that offers several compelling features:

- A unified platform that integrates data engineering, data science, and machine learning. This means you can manage your entire data lifecycle, from ingestion to analysis, all in one place
- Scalability and performance to scale data processing capabilities. It leverages Apache Spark, to handle large datasets efficiently and perform complex computations at high speed and helps reduce costs associated with data processing and storage
- Collaborative notebooks where teams can work together to foster better communication and collaboration among data scientists, analysts, and engineers
- Databricks supports advanced analytics, including real-time data processing and machine learning. It is possible to build, train, and deploy models directly within the platform, making it easier to derive insights and make data-driven decisions
- Databricks integrates with various data sources and tools, including SQL databases, cloud storage, and BI tools. This flexibility ensures you can connect to your existing infrastructure and enhance your data workflows
- Databricks prioritizes data security and compliance, offering features like data encryption and tranched and bespoke levels of access control.

Similarly to Fabric, Databricks meets several UK-relevant compliance standards to ensure data security and privacy, including

- **ISO/IEC 27001:2022**: This certification is for information security management systems (ISMS), ensuring robust security controls and management practices
- **ISO/IEC 27017**: Focuses on cloud-specific security controls, providing guidelines for both service providers and customers
- **ISO/IEC 27018**: Addresses the protection of personal data in the cloud, ensuring privacy and data protection measures

Other Compliance Standards

- **SOC 2 Type II**: Databricks publish that they undergo regular audits to ensure compliance with the Trust Services Criteria for security, availability, and confidentiality
- **PCI DSS**: Databricks supports compliance with the Payment Card Industry Data Security Standard, ensuring secure handling of credit card information

UK-Specific Compliance

- **UK Cyber Essentials Plus (UKCE+)**: Databricks hold certification for protecting against common cyber threats, including enhanced monitoring and encryption

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

This exercise concerns mitigation of a number of risks that are of public concern. NHS fraud is a matter of public concern and the use of data to combat it, particularly when this might concern information about NHS staff and their provision of services – ensuring integrity whilst ensuring that it is applied in an appropriate and proportional matter, are all issues of public concern.

This exercise also concerns public safety; the NHS is one of the largest employers in the world and relies upon the use of mental health workers to maintain its service of care. The delivery of Section 12 care is more transient than other workplace settings, with staff covering multiple organisations and areas; it is therefore important to remain vigilant of this type of fraud risk where dishonest claims provision may be putting patent care in jeopardy. Examples may even extend to unknown, unqualified person has access to patients, staff systems and resources to undertake false Section 12 claims.. This type of fraud can have very serious patient safety implications as well as the financial and reputational risks to NHS organisations.

There is an additional patient safety risk where staff are working multiple shifts and breaching the working time directive (WTD). The WTD is a mandated requirement for all NHS organisations to comply with. This ensures staff have adequate rest between shifts to ensure they can provide safe care to patients. Overworked and tired staff present a risk to patient safety as well as a legal risk/fine if the WTD is breached.

Finally, there is also the political drive to reduce the NHS spend and drive effective spending, in particular as this is linked to poorer patient outcomes and this a drive for efficiency in this space may support improved treatment for patients.

Finally, in terms of the use of data itself, there are relevant public concerns also extend to the protection of data from loss or theft and the controls and oversight for data use itself, to ensure that it is proportional and appropriate. It is for this reason that this DPIA is being undertaken, alongside bespoke Information Sharing Agreements with each participating NHS organisations

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

NHSCFA specific codes of conduct are summarised in the following documents:

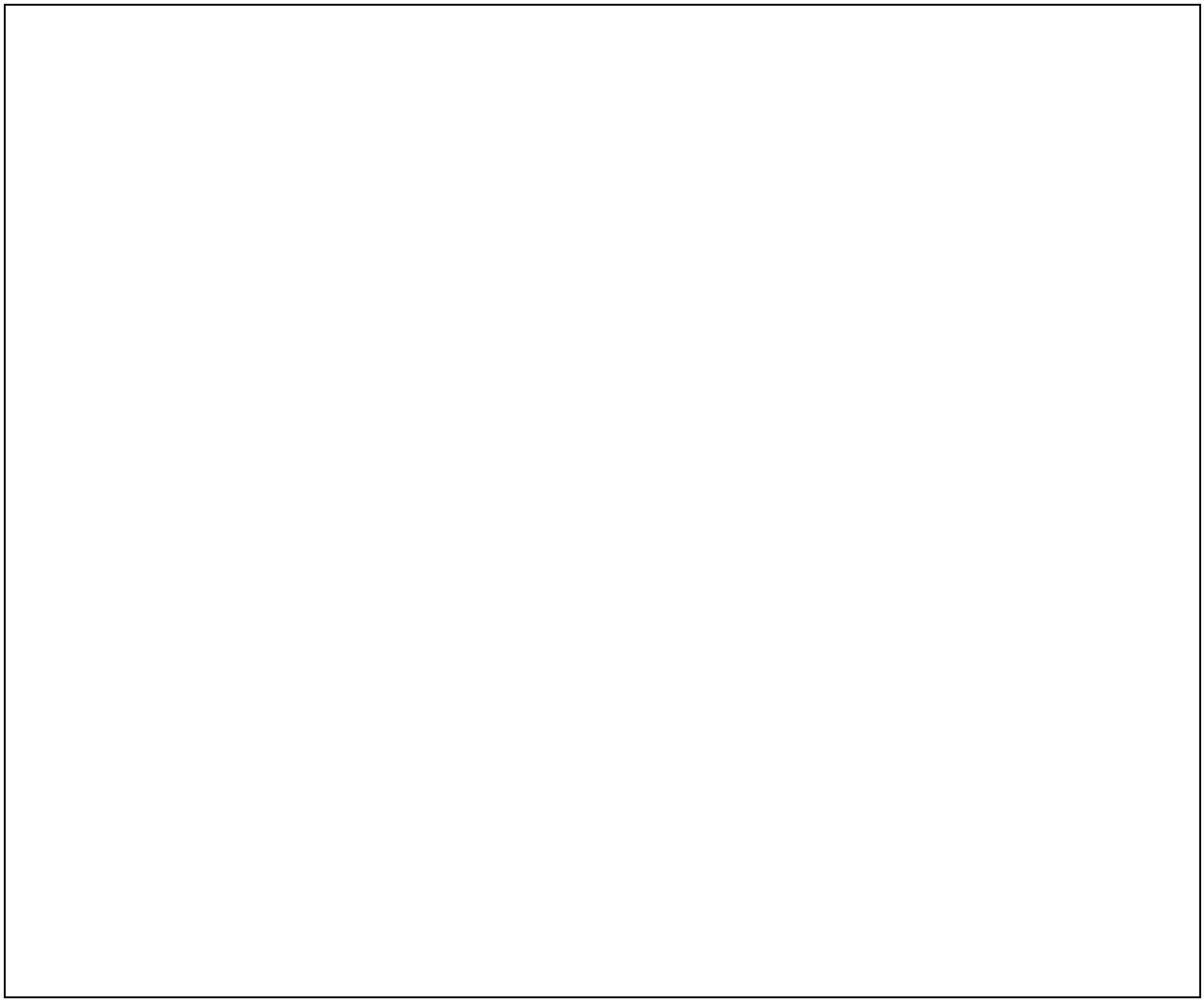
Information Governance:

- 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. (Please add any certification held by supplier)



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?

Broadly speaking, this activity concerns the gathering and use of claims data concerning S12 activity that NHSCFA requires to undertake proactive fraud detection by identifying false claims. This activity supports the NHSCFA's remit of preventing, detecting and investigating fraud, corruption and unlawful activities against or affecting the Health Service in England. By combining domain (subject) specialisms from participants and analytical expertise and technology on a national and local level, this project will substantiate a range of identified fraud risks and increase fraud detection. This, in turn, will provide the opportunities for fraud prevention and enforcement as part of a wider activities drawn from this project, through which NHSCFA and all participating organisations can intervene quickly to reduce the impact and loss from fraud

The main functions of this exercise are therefore:

- Identifying irregular claims patterns which are indicative of fraud.
- Developing processes to identify the scale of fraud and the impact of counter fraud activity.
- Supporting the creation of fraud investigations and informing requirements for more extensive analysis where outliers are detected that may be indicative of fraud
- Identifying, and mitigating, through outlier analysis any system weakness which are identified, for example those which may cause vulnerability to fraud or an inability to detect it.
- Supporting the development and review of policies and procedures to improve governance and mitigate fraud risks.
- Informing and supporting localised awareness campaign lead by the strategic fraud prevention unit focussing on staff fraud to draw attention to the fraud risks and the proactive detection and prevention being undertaken
- Driving behavioural change through all the above, dissuading dishonest practice by raising the likelihood of being detected, ideally generating quantifiable outcomes for future remeasurement of decreased outliers.

2. What is the intended effect on individuals?

The pilot is designed to inform whether fraudulent activity exists within the S12 database by utilising claims data concerning a range of recognized fraud types. It will identify the existence of suspected false claims, and to what extent such fraudulent activity presents a risk to the NHS by determining the scale and scope of such activities. This analysis must be undertaken through a data share between the participating NHS Organisations and NHSCFA, as it is necessary to match claimants data - however beyond the processing of the S12 data (i.e. that they have claimed to have attend at a certain time and location in sanctioned NHS activities) no further information is needed.

In circumstances where any individual outlier can identify, this exercise can be utilised to support further action which may culminate into investigations against individuals and subsequent. Individual outliers can be identified and then the information would be diverted to a 'business as usual' process for national or local investigation, with the outcome being recorded and utilised in terms of any criminal or civil sanctions achieved and any funds recovered.

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

As an individual, there are no benefits for this processing.

More broadly, processing this data serves the prevention and detection of crime. More specifically to the NHS remit of the NHSCFA, the benefits serve effective protection of public services and effective management of the public purse and thus overwhelmingly falls within the public interest.

STEP 3: Consultation process

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?

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

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?

Because the nature of this processing concerns cases of suspected fraud, as well as the methods and mechanisms used to detect it, it is often not possible or appropriate to engage with data subjects as these may be the subject of scrutiny. However, in support of these types of data shares, NHSCFA has historically engaged with a range of stakeholders, including with the National Data Guardian within consultations and workshops that concerned the use of personal data for fraud detection within healthcare, which included representatives of patient groups.

This project is supported by the expertise of the participating NHS organisation, who employ key individuals who can provide domain knowledge to support the activity and validate findings.

NHSCFA also makes use of extensive online resources to outline the use of data and the approach taken and ensure transparency in terms of the application of data, as well as the estimated extent of designated fraud risks.

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

The approach for analysis is drawn from a wealth of in-house expertise concerning data science, supported by intelligence and operational knowledge that is linked to fraud investigation. Additionally, the technological, information security and wider IT considerations are supported by a Technology Team with sufficient knowledge. Additionally, there are robust mechanisms for oversight in terms of Information Governance, wider corporate governance mechanisms which necessitate compliance and, finally, the existence of oversight groups such as the Data Strategy Group which can take decisions and approve /reject submissions concerning the application of data and the mechanisms for recording their outcome.

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

The circumstances for engagement are individual to each participating organisation and the way they commission and pay for their mental health services - this is partially pertinent as the Section 12 services, which may overlap in terms of funding and have variations in terms of who acts as Data Controller and Data Processor in each instance. For these reasons, individual Information Sharing Agreements will be put in place for each individual share that outlines the respective roles of each party as individual participants and also within the context of the wider project.

However, beyond this there should be no need for wider participation from third parties. Following the data share, there are no identified circumstances where wider / 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.

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

The appropriate expertise is sourced in house through designated resources and expertise provided by the appropriate departments and deemed adequate, in particular due to the compliance

mechanisms achieved with regulatory Information security standards such as the ISO/IEC 27000 family.

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?

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

Article 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.

Article 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 we are relying on for this data sharing, which is 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;

2. Does the processing actually achieve your purpose?

This can be confirmed, because this data share is the extension of a previous exercise undertaken in a single organisational s a piece of reactive activities, which was able to determine sufficient outliers to warrant extending it into the proactive space.

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

The exercise entails combining the S12 data from a range of organisations (the participating NHS Trusts) and applying data capability and expertise from the NHSCFA – as such, no alternatives are possible to attain the outcomes of this exercise.

4. How will you prevent function creep?

Function creep can be prevented by incorporating it within the existing control and mechanisms for proactive counter fraud prevention and also through the development of the business case and Data Sharing Agreements which articulate the intentions, to a sufficient level of detail, and provide a basis for continued engagement with the participating organisations, to allow transparency and oversight in the project and its outcomes.

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?

The data selected has been identified as them minimum necessary to undertake the task. Information is provided the participating NHS organisations by individual NHS-funded Mental health contractors to populate the S12 claims reporting system and there are a range of validation and verification processes that control the format and content of the data. Each participating NHS organisation, in their role as data controller, are responsible for the accuracy of gathered data, for both their own records and additionally for information provided to NHSCFA within this data share. Because NHSCFA has no means to audit or review this data for accuracy, it is accepted that this must be used with caution.

Outlier detection, by its nature, identifies inaccuracies and this is intrinsic to the data science framework and the validation process necessary to determine whether fraud has occurred. Information which is subsequently used to support fraud investigations will be assessed against other

records and forms of evidence for accuracy as part of the case management process for fraud investigations.

6. What information will you give individuals?

NHS Counter Fraud Authority has a Privacy Statement that outlines the extent of the intended use of data including that which is personally identifiable. It provides a mechanism to engage directly NHSCFA to find out more. As such, this exercise is being drawn together with this in mind to ensure that any risk would be mitigated through robust controls and transparency in terms of the application and use of data.

IN terms of that provided directly by the participating NHS organisation, , there are notifications within the S12 software, as well as wider privacy notices, that identify that data will be subject for scrutiny for counter fraud purposes, although the extent they are utilised will be individual to each participating organisation

It is less likely that it would be expected that this activity would need to be facilitated via a data share and so, as part of the opt-in process and information sharing protocols within each organisation, recommendations will be made to consider the current and potential notification of staff (this, in turn, will act as a form of disruption) to the extent that, as Data Controller, they are satisfied that their responsibilities are met

7. How will you help to support their rights?

To support the rights of individuals whose data is being shared, the data will be treated as personal sensitive data, however in reality this is not likely to be present (it simply concerns the inability to control “free text” fields. This also supersedes the requirements for managing the personally indefinable data that IS included. Accordingly, appropriately secure methods of transfer will be used when sharing the data, and it will only be shared with parties where necessary (as outlined by the InformatioN Sharing agreement, which stipulates that “No disclosable information shall be transmitted unless by encrypted and/or password secured means.”. Each match will be ranked by its strength to inform any decisions made around the further investigation of the data and, in any event, the data will either remain within the NHSCFA for management by the National Investigation Team, or disseminated back to the NHS organisation who produced the data in the first instance (and who themselves receive the data matches).

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

This particulars of this exercise are managed by individual Information Sharing Agreement which all parties will agree to as part of their joining the exercise, it stipulates agreed conditions for all elements of this data share.

Additionally, there are robust mechanisms for oversight in terms of Information Governance, wider corporate governance mechanisms which necessitate compliance and, finally, the existence of oversight groups such as the Data Strategy Group which can take decisions and approve /reject submissions concerning the application of data and the mechanisms for recording their outcome.

9. How do you safeguard any international transfers?

There is no intention to extend this transfer this data over international boundaries, nor extend it to any processors beyond those outlined in the paragraph above.

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	Remote	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
8. There is a risk that information could be lost, released or shared inappropriately	Remote	Significant	Medium
9. There is a risk that processing is carried out in a territory without appropriate personal data protection	Remote	Minimal	Low
10. There is a risk that creditors will be misidentified as a result of data processing	Possible	Significant	Medium

There is a risk that the quality of data will not be to a consistently high standard	Possible	Significant	Medium

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved by SMT Owner Yes/No
(1) There is a risk that sensitive data will be used for purposes other than that which are stipulated in the business case	(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 unnecessary personal data from the structured data, ensure that all possible steps have been taken to ensure the inclusion of personal data is appropriate and necessary for the project.	Low	Yes - TM
(2) There is a risk that complex processing of data by participating authorities may lead to information being inadvertently disclosed.		Low	Yes - TM
(3) There is a risk that incorrect information may be disclosed by participating authorities during the pilot (leading to incorrect identification of fraud)		Low	Yes - TM
(4) There is a risk that incorrect information may be disclosed to unauthorised parties	(4) Data quality review is undertaken by authorities sharing data to review individuals / organisations included and remove irrelevant ones from the matching process.	Low	Yes - TM
(5) There is a risk that data is retained for longer than it is needed	Each data source is subject to a range of mapping and corresponding retention schedule. Deletion is undertaken manually, with human oversight.	Low	Yes - TM

(6) There is a risk that individual's rights under GDPR are violated	(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	Low	Yes - TM
(7) There is a risk that an external attacker gains access to personal data	(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.	Low	Yes - TM
(8) There is a risk that information could be lost, released or shared inappropriately	(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.	Low	Yes - TM
(10) There is a risk that individuals could be misidentified as a result of data processing.	(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 Data Platform will be assessed to manage false positives and triage follow up investigations.	Low	Yes - TM

(11) There is a risk that the quality of data will not be to a consistently high standard	(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.	Low	Yes - TM

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by SMT Owner:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by SMT Owner:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice: Having reviewed the DPIA I am satisfied that a comprehensive assessment has been undertaken of the NHSCFA secure environment, where the data relating to 'Section 12' exercise will be stored and analysed, specifically Microsoft Fabric and DataBricks. Primary analytical access will be restricted to approximately 12 members of staff which includes Data Scientists and Data Engineers with permission role-based access, therefore making it fully auditable. The Data Analytics Platform upon which the data is accessed and utilised has a separate DPIA. This platform has direct interconnections with other NHSCFA systems and applications, each of these have their own access control measures and controls in place to mitigate any risk of unauthorised access. 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.		
DPO advice accepted or overruled by:		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	

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The impact level of the s12 Local Exercise was assessed as OFFICIAL
2. The following measures briefly describe what controls have been implemented and the personal data recorded:
    a. Upon receipt by NHSCFA, the data concerned for analysis is primarily accessed by approximately 12 members of staff from NHSCFA, which includes the Data Scientists and Data Engineers. However, outputs and wider data disseminations are specific to individual projects and their designated outcomes.
    b. The Data Analytics Platform upon which the dental data is accessed and utilised has a separate DPIA. This 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.
    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 s12 Local Exercise.
4. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

5. The participating NHS organisations have responsibility for the administration of the S12 Database/System and NHSCFA has responsibility for the data following receipt and this storage and use in line with this DPIA and the Information Sharing Agreement. 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 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 Database/System is summarised in Appendix A

7. This data includes personally identifiable data, but no sensitive data is processed.

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 S12 Local Data Exercise 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. The data sourced for the S12 Data Exercise is to support local work. Therefore findings will be shared internally with NHSCFA data experts and other specialists in the following context

- Sharing findings (outliers) internally for the purposes of utilizing domain expertise for verification/.validation.
- Analysts will utilize data to undertake analysis to determine outliers in order to determine and identify outliers which could be indicative of fraud.
- Depending on the findings themselves, the basis for sharing and processing the data and the strength of the outliers, it is possible that the outliers may be shared with NHSCFA's own investigative services for further action (i.e. In support of more specificr data sharing agreement under BAU)
- Information Analysts produce a data-based output, for example an electronic dashboard or statistical physical report detailing output and findings, that is utilized to support a summary of the NHSCFA activity and outputs which may contain sample, aggregated or summarized excerpts of the data.

Section 5: External Sharing and Disclosure of Data

13. The only information shared with external organisations, would be in terms of sharing the findings with the participating NHS Organisations and engaging in order to validate the activity and/or outcomes. This would be in accordance with appropriate Information Sharing Agreement

Section 6: Notice/Signage

15. 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 and provides contact details to contact NHSCFA in any capacity (or to make an information request)

16. 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.

17. 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.

18. In terms of direct notification, there are notices and statements within the S12 software, as well as wider privacy notices employed by participating NHS organisations, that identify that data will be subject for scrutiny for counter fraud purposes, although the extent they are utilised will be individual to each participating organisation.

19. As part of the opt-in process and information sharing protocols within each organisation, recommendations will be made to consider the current and potential notification of staff (this, in turn, will act as a form of disruption) to the extent that, as Data Controller, they are satisfied that their responsibilities are met

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

Right to Access

20. 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. It is unlikely that many access requests will be received as the personal data recorded is primarily held by participating NHS Organisations.

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

22. Were NHSCFA or the participating NHS organisations be subject to a request for deletion by a data subject who wishes their data amended or 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.

23. 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

24. 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.

25. 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 and the participating NHS Organisation 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.

26. It would be necessary to document the considerations and outcomes and may also be possible to give assurance through the extent that NHSCFA already partly comply with this request through use of the masking techniques. However, the answers above provide a generic response, which may not encapsulate wider reasons 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 and the hosting infrastructure is subject to the ISO27000 and ISO27001.

28. Access 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

3. Information Governance Policy
4. Information breach Reporting Policy
5. Data Quality Policy
6. GDPR – Data Protection Policy
7. Information Security Policy
8. NHSCFA Acceptable use Policy

31. The Data Analytical platform has its own additional DPIA which provides further information specific to the technology and should be sourced for specific information relating to the software and how it is applied.

9. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the exercise, and the personal data that it concerns, 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.

The Privacy and Electronic Communications Regulations

4. 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

5. 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

6. 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

7. There are no residual privacy risks to the personal data recorded in the Database/System. 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	NHSCFA Project Athena
Project	S12 Local Exercise

2. Contact position and/or name.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Data Protection Officer
Branch / Division	Finance and Corporate Governance, NHSCFA

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 primary purpose of this exercise concerns data drawn from the S12 Solutions platform that is gathered by a number of participating NHS organisations which will be collected by NHSCFA and used for proactive data analysis. This tool records information concerning Mental Health Assessments and the clinicians undertaking them, in particular the Approved Mental Health Professionals (AMHPs) with Section 12 doctors. Through use of proactive data analytics undertaken by NHSCFA against the submitted Electronic Claim Forms the intention is to detect false claims and other outliers that can be indicative of fraud. This has been identified through reactive work undertaken by NHSCFA and this exercise is intended to be a proof-of-concept that widens the scope of this work through a proactive exercise with additional organisations, designed to identify deviant patterns of behaviour on a larger scale. This data share concerns [personally identifiable data concerning mental health professionals and their claimed date/time/location of mental health services.

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. In this instance, the exercise is an extension of a single reactive exercise into a proactive space and the collaboration of NHSCFA and a range of NHS organisations to share their data to allow NHSCFA data capabilities and expertise to be applied.

NHSCFA remit from the 2017 Secretary Of State Directions supports data sharing in pursuit of fraud and supports NHS Bodies / Special Health Authorities in providing data. This approach is also supported by legislation Data Protection Act 2018 (DPA) Schedule 8, sections 1 and 8 (i.e. necessary for enactment of rule of law, in substantial public interest, necessary for the purposes of preventing fraud or a particular kind of fraud,

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

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data needed for the exercise. The personal data implication concern the identity of clinicians making claims from the NHS for their services, those approving it, as well as anonymised patient data (initials) to act as means for distinction. It is recognised that the requirement is minimised as the necessary required to undertake this exercise.

Data will be gathered for a specific, justifiable and proportional purpose 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 the first DPIA carried out on this S12 exercise.

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.

Appendix A – Section 12 Claims Data Specification

Below is a summary of the data specifications required from the S12 claims process (whether from the S12 software or collated from claims forms). Due to the universal nature of the S12 claims form, this will be the same in each instance, regardless of the originating NHS organisation

Field Name	Type	PID?
Claim ID	Number	N
Doctor Name	Text	Y
Doctor Contact Details	Text	N
Authorised By	Text	Y
Authorisation Date	Date	N
Claim Status	Text	N
Approver	Text	Y
CCG Relation	Text	N
CCG Related Location	Text	N
Visit Date	Date	N
Visit Time	Time	N
ICB	Text	N
Patient Initials	Text	N *

NHSCFA offices

Coventry

9th Floor
Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

Paid?	Y/N	N
Approved Date	Date	N
Paid Date	Date	N
Mileage	Number	N
From	Text	N
To	Text	N
Additional Expenses	Number	N
Mileage Amount	Number	N
Report Amount	Number	N
Employer	Text	N
Amount Paid	Number	N

*The patient initials are required as a means to ensure distinctiveness and separate duplicate claims from multiple attendance, however because the initials themselves are insufficient to identify the patient, either directly or indirectly, from the wider information in this dataset (or any wider data held by NHSCFA) this is considered as anonymised.

NHSCFA offices

Coventry

9th Floor
Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

Page left intentionally blank.

NHSCFA offices

Coventry

9th Floor
Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH