NHS
Counter Fraud Authority

GP Flu Vaccinations Loss Analysis Database

Data Protection Impact Assessment

September 2021

V1.0 Published

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

Executive Summary

This document contains information in relation to *GP Flu Vaccinations Loss Analysis Database*

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'**

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Senior Loss Analysis Specialist	DPIA GP Flu Vaccinations Loss Analysis Database	DPO	V0.1	11/08/2021	Initial creation
Senior Loss Analysis Specialist	DPIA GP Flu Vaccinations Loss Analysis Database	DPO	V0.2	19/08/2021	SMT review
Senior Loss Analysis Specialist	DPIA GP Flu Vaccinations Loss Analysis Database	DPO	V1.0	14/09/2021	Amended and saved as Published

Prefix	
Reference:	**DPIA** **GP Flu Vaccinations Loss Analysis Database**
Date:	**14/09/2021**
Author:	**Senior Loss Analysis Specialist**
Data Owner:	**Strategic Intelligence Lead**
Version:	**1.0**
Supersedes	**0.2**

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.

[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.

GP Flu Vaccinations Loss Analysis Database

General Description

10. The GP flu vaccinations loss analysis database is the working Microsoft Access database for a loss analysis exercise looking to validate claims made by GPs for administering flu vaccinations to eligible patients. The database will contain details of patients who are recorded as having received flu vaccinations and details of the GPs who submitted the claims. All four members of NHSCFA strategic intelligence staff working on the loss analysis exercise will have access to the database.

11. The following categories of data may be stored in the database: patient personal details, including personally identifiable data, vaccination details, GP details and details of claims for payment or reimbursement. The data will be collected by large volume exchange of electronic data from GP systems to NHSCFA using password protected Microsoft Excel via Egress secure file transfer, which will be copied or uploaded to the Microsoft Access database. Data will also be manually input into the database during the course of the loss analysis exercise.

12. This is the first DPIA to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with the Senior Loss Analysis Specialist and the Information Governance and Risk Management Lead.

13. The GP Flu Vaccinations Loss Analysis Database 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

14. To ensure the Database 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

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

[2] Version 0.3 (20180209)

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 GP Flu Vaccinations Loss Analysis exercise aims to check and validate claims made by GPs for providing seasonal flu vaccinations, with a view to producing some benchmark loss estimate figures in this area. Losses can occur when a contractor wrongfully claims for an NHS service that was not provided, that cannot be substantiated, that did not comply with the rules on service provision or service specification, or that was not clinically needed, by way of false representation, by failing to disclose information and/or by abuse of position. Losses can also occur where the contractor makes a genuine mistake when claiming for a service. The exercise will contact patients who, according to records submitted to NHS England and Improvement (NHSE&I) and/or NHS Business Services Authority (NHSBSA), received an NHS funded seasonal flu vaccination, and ask patients to confirm their experience of the service received. The exercise will also be checking and validating patient eligibility for an NHS funded seasonal flu vaccination with the relevant authorities. This loss analysis exercise has been commissioned by the NHS Counter Fraud Board, comprising NHS Counter Fraud Authority, NHS England and Improvement, NHS Business Services Authority, Department of Health and Social Care and the Cabinet Office. The requirement to conduct a DPIA has been identified within the initial project plan to ensure the highest levels of governance and protection are applied to the project data prior to processing. Once data for the project comes through, we will hold a large amount of person identifiable and sensitive/special category data that will be used to support decision making. At this point, our intention will be to process the data on a routine basis to confirm details, to check for patterns and behaviours, and to produce key statistics. It is the protection of this data in its raw format that has mainly prompted the DPIA. In addition, we want to provide assurance to the organisation that we are processing this data in a safe, legal and ethical way that supports the core obligations of the business.

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)

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

1. Data will consist of electronic data, relating to flu vaccinations administered to patients during the 2020-2021 flu season, extracted from a random sample of 200 GP practice systems. The data will be emailed to NHSCFA in password protected Microsoft Excel format using Egress secure file transfer. Once received, the data will be copied or uploaded into a bespoke Microsoft Access database, which is the subject of this DPIA. The Access database and original Excel files will be held on a secure server. Additional supporting data will be supplied electronically by NHSE&I and NHSBSA, relating to claims for fees and reimbursements associated with the flu vaccinations. Other supporting information relating to the flu vaccinations will be provided by patients in hard copy format, by way of completed questionnaires returned to NHSCFA, which will be manually added to the project database.

   All data received will be processed, retained and erased according to the NHSCFA Data Retention policy and in strict accordance with the Data Protection Act 2018 and the GDPR. All data obtained will be stored in a secure project database, held on a secure server, and/or in paper format maintained at a secure location. NHSCFA operates a clear desk policy, which means all sensitive or personal data (when not being processed) will be locked away in a secure area. Any surplus data, data not selected as part of the exercise sample, data which does not serve any purpose, or data obtained in error will be returned to their source and/or deleted from our files.

   All data selected for the exercise will be held solely for the duration of the exercise, for the production of reports and to allow sufficient opportunity for an audit of the exercise to be completed should an audit be required. Once the project and any audits are complete, all data (both electronic and hard copy format) will either be returned to their source and/or deleted from our files and/or disposed of as confidential waste.

2. The main sources of data will be GP practices, NHSE&I claims processing systems, NHSBSA claims processing systems, patients. Other sources of information include the NHS Summary Care Record (SCR) database and the General Medical Council (GMC) professional register, as well as sources which are openly accessible such as the internet and social media sites.

3. Data obtained from GPs on flu vaccinations will be shared with the patients who are named on the vaccination record, for them to confirm they received the vaccine and to validate details of the vaccination. NHSCFA may be required to share data with other organisations in order to carry out essential validation checks and fulfil our statutory duties in relation to loss analysis, in which case this data will be shared under a memorandum of understanding or other legal gateway. Other organisations may include NHS bodies or healthcare organisations providing a service to the NHS, NHS processing bodies, such as NHSE&I, NHSBSA or NHSSBS, the police, law enforcement agencies, regulatory bodies, government departments such as DWP or HMRC.

4. Potential 'high risk' processing includes potential data breaches caused by uncontrolled exchange of data and potential misrepresentation caused by any incorrect or inaccurate data. Uncontrolled exchange of data has been minimised by introducing a single point of entry into NHSCFA for the data to be emailed, and using password protected spreadsheets and Egress secure file transfer, thereby preventing multiple exchanges to different recipients, which is an improvement to business processes. Upon receipt of the data, it will be checked, validated and where necessary corrected, in order to identify and rectify any incorrect or inaccurate information prior to onward processing.

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. The data required for the project will comprise GP records for delivering flu vaccinations and the associated item of service claim and, if applicable, reimbursement claim. The records will consist of: flu vaccination record unique identifier; GP practice code; practice name and address; NHS England team; patient NHS number; patient name; patient address; patient date of birth; patient death status; patient date of death (if applicable); date flu vaccine administered; venue where flu vaccination took place; vaccine product used; name and professional registration number of the person who administered the vaccine; patient eligibility cohort group; item of service claim unique identifier; date item of service claim submitted; date item of service payment made; item of service payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the item of service claim; reimbursement claim unique identifier; date reimbursement claim submitted; name of vaccine product; date reimbursement payment made; reimbursement payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the reimbursement claim.

   The required data includes the patient's NHS number and clinical details of their flu vaccination. These are essential in order that they be checked and verified, in order to confirm the GP has submitted a legitimate claim for item of service fees and reimbursement of the vaccine. The data does not include any criminal offence information.

2. In order to compare and verify monthly declared counts, and to avoid GPs cherry picking flu vaccination records, for each of the 200 GP contractors, we need data for all the flu vaccinations they administered each month for the 2020-2021 flu vaccination season. The average number of records per GP for the entire flu season is around 2,871 each, which means the initial data request will comprise around 574,200 records. A number of essential validation checks will be carried out on the whole dataset before a random sample of 5,000 records will be chosen for the next stage of the exercise. At this stage, records not selected as part of the 5,000 sample will be deleted from our files.

3. This is a one off data request for a bespoke loss analysis exercise. Data will be requested at the beginning of September 2021, and GPs will have six weeks to provide it.

4. It is envisaged that the loss analysis exercise will commence in September 2021 and conclude at the end of March 2022. Set-up, data cleansing and re-formatting, initial validation checks and fieldwork will take approximately 17 weeks to complete with 22 weeks allocated to data analysis, decision making, results and statistical outcomes, and the production of a project report, although some of this time will overlap as the exercise progresses. Data will be kept from the beginning of September 2021 until the project concludes, and then for a further six months after completion (to the end of September 2022) to facilitate any audit requirements.

5. The initial data request will comprise around 574,200 records relating to flu vaccinations, although some patients might feature more than once. For the later stages of the exercise, a sample of 5,000 records will be selected with the other records deleted from the files.

6. The exercise covers all regions of England only.

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. There is no direct relationship. The data subjects for the loss analysis exercise are randomly selected from all flu vaccination claims made by GPs during the 2020-2021 flu season.

2. As the information will be required for a loss analysis exercise, one of NHSCFA's statutory functions, there are exemptions under the DPA for research, which means the rights of data subjects are limited. Data subjects randomly selected for the exercise are unlikely to be aware that we are processing their data until they are contacted to complete a questionnaire and as such will not have control of their data.

3. On receipt of an NHS funded flu vaccination, patients give consent for their data to be used for post payment verification purposes, amongst other purposes. Post payment verification is a process designed to ensure the GP receives the correct fees and reimbursements for providing an NHS service. Part of this process involves confirming service delivery with patients named on records used by GPs to claim payments. This loss analysis exercise is essentially a post payment verification exercise designed to confirm service delivery and identify any inappropriate claims by GPs. Data subjects would expect their data to be processed by NHSCFA for this purpose.

4. The eligibility groups for NHS funded flu vaccinations include children, the elderly and people with complex medical needs, so the randomly selected sample for the loss analysis exercise will include children and vulnerable groups.

5. Potential 'security flaws' within processing include potential data breaches caused by uncontrolled exchange of data and potential misrepresentation caused by any incorrect or inaccurate data. Uncontrolled exchange of data has been minimised by introducing a single point of entry into NHSCFA for the data to be emailed, and using password protected spreadsheets and Egress secure file transfer, thereby preventing multiple exchanges to different recipients, which is an improvement to business processes. Upon receipt of the data, it will be checked, validated and where necessary corrected, in order to identify and rectify any incorrect or inaccurate information prior to onward processing.

6. This is not novel for NHSCFA or the industry. Recording data on a bespoke loss analysis database is standard practice that has been carried out on several previous occasions by NHSCFA on other loss analysis exercises.

7. Technology in this area has evolved slightly over time, with greater use made of electronic data rather than paper-based data. Electronic data will be emailed to NHSCFA in password protected Microsoft Excel format using Egress secure file transfer. Once received, the data will be copied or uploaded into a bespoke Microsoft Access database, which is the subject of this DPIA. The Access database and original Excel files will be held on a secure server. Additional supporting data will be supplied electronically by NHSE&I and NHSBSA, relating to claims for fees and reimbursements

associated with the flu vaccinations. Other supporting information relating to the flu vaccinations will be provided by patients in hard copy format, by way of completed questionnaires returned to NHSCFA, which will be manually added to the project database.

8. There are no issues of public concern. As with all NHSCFA loss analysis exercises involving patient data, all information will be obtained, stored and handled in accordance with the DPA and GDPR, acceptable use policy, standards of business conduct and policies relating to information sharing. The loss analysis exercise will support the production of loss estimates and identify key areas of vulnerability within the flu vaccination service. The exercise will therefore satisfy any need to respond to FOI queries for questions relating to the subject matter of the exercise.

9. 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. To identify the nature and scale of inappropriate GP claims for providing NHS funded flu vaccination services. To produce estimates of loss within the NHS flu vaccination service.

2. No impact on individuals, but this may support the development of appropriate policies and procedures to help eliminate vulnerabilities and reduce losses within the NHS flu vaccination service. It is not the intention of the exercise for NHSCFA to take action against GPs whose claims for flu vaccinations are deemed to be inappropriate, as the data was not sought for this purpose.

3. Successful completion of the loss analysis exercise will be of benefit to me in my role as Senior Loss Analysis Specialist and to the Strategic Intelligence Team, by identifying and estimating NHS revenue lost to fraud and inappropriate claiming. The results of the loss analysis exercise will count towards NHSCFA's financial target of £400 million fraud prevention recoveries to the NHS. The exercise might also count towards NHSCFA's contribution to the Cabinet Office fraud measurement programme.

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. From initial contemplation of a loss analysis exercise looking at claims for flu vaccination services, a working group was formed to discuss the merits and feasibility of such an exercise. The working group is made up of experts and specialists from different sectors of the health service, each with a professional interest in seeing such an exercise succeed. Alongside NHSCFA, member organisations include NHSE&I, NHSBSA and DHSC. The working group have met on a number of occasions to discuss and agree the scope and aims of the exercise, the terms and conditions, data sampling and the methodology to be used. The working group will be kept up to date on a regular basis as to progress of the exercise and all claims considered to be 'inappropriate' will be put before the working group for final consideration.

2. In preparation for this exercise, the Senior Loss Analysis Specialist has been in consultation with other teams within NHSCFA as to what requirements are needed to make the exercise a success, including other members of the Strategic Intelligence Team, the Data Analytics Team, the Fraud Prevention Team, the Information Governance Team and the Senior Management Team.

3. Yes, processors will be part of the Loss Analysis Team.

4. Yes, internal consultation with NHSCFA Information Governance Team and external consultation with NHSBSA and NHSE&I to discuss arrangements for the secure transfer and storage of data.

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. Public Task – For the prevention and detection of crime against the NHS. The lawful basis for processing are set out in Article 6 of the GDPR, which states that 'the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law'.

2. Yes.

3. No. The exercise relies on contacting patients who are recorded on GP claims for fees and reimbursements as having received an NHS funded flu vaccine and asking them to confirm this and other details of the service. Without being able to trace and contact patients, a large proportion of known fraud risks would remain unchecked.

4. The parameters of the exercise and processing needs are limited to specific use. NHSCFA receive training throughout the year on DPA and GDPR and the use of data for its collected purpose. We will prevent function creep by keeping our processing under periodic review. We do not expect the purpose of processing to change following completion of the loss analysis exercise.

5. The majority of fields within the loss analysis database will be limited to set values in a multiple choice format to prevent inaccuracies caused by admin error. The checking of information in a loss analysis exercise, where contact with data subjects is required, can be challenging due to the free text nature of information collected, ruling out automated checking and validation on the majority of fields. Where information is manually entered into the project database, this can be checked for quality, accuracy and minimisation as it is being processed. Data within the database is regularly reviewed by members of the loss analysis team in order for judgements to be made and decisions reached, so data can be checked for quality, accuracy and minimisation as it is being reviewed. Reports can be run from the database to identify information that may be incorrect such as dates in the future. Retention reviews will be undertaken to limit the time the information is held for. Information collected for the purposes of the prevention and detection of crime will have to be considered for necessity and proportionality. However, due to some legislative requirements, it may be necessary to retain some data which may not appear relevant.

6. Individuals can make requests to the NHSCFA by a subject access request. This is considered by the Information Governance team and a decision is made on what information to release. Due to the type of processing, a data subject's rights may be limited. How we handle personal data, our

legal basis for processing and who we work with and may share data with is outlined in the NHSCFA privacy policy.

7. The NHSCFA privacy policy explains the rights of data subjects subject to relevant exemptions and the process to be followed. NHSCFA will help support the rights of data subjects by ensuring compliance with the DPA and GDPR, protecting personal data and its integrity, ensuring governance is applied at key stages without minimising the operational need to process the data. NHSCFA has a range of policies and procedures in place for maintaining compliance with DPA and GDPR and a range of safeguards for retaining data securely against cyber attacks, including ISO27001 accreditation and audit arrangements.

8. We will periodically seek assurance from data providers of their continued compliance with applicable data protection rules, and we will work closely with information security and information governance colleagues to flag up and address any concerns. The Senior Loss Analysis Specialist and Performance and Improvement Lead will ensure that all applicable Standard Operating Procedures are observed and followed by data processors. The Information Security Management System has attained ISO 27001 accreditation, the parameters of which data processors must comply.

9. There is no requirement to conduct international transfers of data supplied for this loss analysis exercise. Data will not be transferred outside the UK.

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
There is a risk of data breach involving disclosure of potentially sensitive data relating to a patient's GP and flu vaccination treatment.	Possible	Significant	Low
There is a risk that the personal data is used for purposes other than for what it was originally intended for, for example to take action against individuals suspected of perpetrating a fraud.	Possible	Significant	Low
There is a risk that personal data is retained for longer than necessary contrary to data retention policies and best practice.	Possible	Minimal	Low
There is a risk that the personal data is no longer relevant.	Remote	Minimal	Low
There is a risk that the personal data is not accurate or up to date. Procedures are in place to check, validate and where necessary update information.	Remote	Minimal	Low
There is a risk that the confidentiality of the personal data is not adequately protected.	Possible	Minimal	Low
There is a risk that personal data is passed unauthorised to external organisations.	Possible	Significant	Low
There is a risk of hosting server failure. In addition to nightly backups, the database servers offer a point in time recovery that means that there is minimal loss of data in the event that data recovery is necessary. As part of our business continuity testing, we have been able to fully restore services within two hours.	Possible	Minimal	Low
There is a risk of IT failure due to events such as fire, flooding, force majeure. The use of the AWS facilities ensure that IT failures due to environmental and power outages are extremely low.	Remote	Significant	Low
There is a risk that data held is accessed by cyber criminals. The required mitigations are in place to ensure data security including virus protection, system monitoring and vulnerability patching.	Remote	Severe	Low

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
Users are only given sufficient rights to systems to enable them to perform their specific job function. User rights will be kept to the minimum required to do their job effectively and efficiently. Access rights are reviewed on a monthly basis and controls are placed on how much information can be exported to be used for other purposes.	Reduced	Low	RWH 19/08/2021
This DPIA exists to ensure that there is due consideration as to the extent of the data used. Processors also have to consider the proportionality and justification for all information that they look to collect initially. Information is also reviewed by Information Governance colleagues and senior managers so that any issues can be highlighted to the Senior Loss Analysis Specialist to rectify and avoid in the future.	Reduced	Low	RWH 19/08/2021
The loss analysis database is subject to the NHSCFA Data Handling and Storage Policy and is audited regularly to ensure that personal data is not retained for longer than is necessary.	Reduced	Low	RWH 19/08/2021
Relevance of personal data is one of the aspects considered during the review. Given that the personal data gathered is always specific to a loss analysis exercise aimed to identify the nature and scale of fraud, the data will always be relevant as individually it provides a case study of instances of fraud and in bulk it can be used to profile perpetrators and produce loss estimates and trends in relation to fraud within the NHS.	Reduced	Low	RWH 19/08/2021
Data for loss analysis exercises is provided by various sources and updated as the exercise progresses. As such, the responsibility for accuracy lies with the responsible officer for the report. Where possible checks are made to corroborate information. The application interfaces within the loss analysis database can be used to identify obvious mistakes such as transposition errors when entering data manually.	Accepted	Low	RWH 19/08/2021
The loss analysis database is protected by a multifactor authentication protected system which requires a username, a password and a device known	Reduced	Low	RWH

to the user in order to gain access to the network and reach the database. Permissions for the database are allocated to staff on a role and organisation basis so that they only see personal information which is required for their role.			19/08/2021
Requests by other agencies need to be made in writing to the NHSCFA. Officers determine whether the request is proportional or necessary before releasing the information. It may be necessary to release information to external agencies such as other law enforcement agencies, government departments or regulatory bodies to verify information and carry out functions designed to protect the public.	Accepted	Low	RWH 19/08/2021

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 of the access, storage and subsequent retention of person identifiable data obtained from GP systems and transferred to NHSCFA using password protected Microsoft Excel via Egress secure file transfer has been carried out. Access and the use of the data will be limited to only that required to achieve the stated purposes, with access restricted only to those members of the Strategic Intelligence team working on the loss analysis exercise. Access 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.		
DPO advice accepted or overruled by:	Trevor Duplessis - 14th September 2021	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)	Intelligence and Research Development Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Senior Loss Analysis Specialist
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Data Maintenance and Protection Overview

1. The GP flu vaccinations loss analysis database is a database which will facilitate a loss analysis exercise looking at claims for flu vaccination services.
2. The categories of data that may be stored in the database are: Patient personal details, including person identifiable, GP details and details of flu vaccination treatments received.
3. The impact level of the GP flu vaccinations loss analysis database was assessed as OFFICIAL SENSITIVE and it can only be accessed internally.
4. The following measures briefly describe what controls have been implemented to protect the database and the personal data recorded:
    a. The database is accessed by approximately 4 members of staff from NHSCFA, which includes the database administrators.
    b. The database does not have any direct interconnections with other NHSCFA systems and applications.
    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.
5. It is assessed that there are no residual privacy risks to the personal data used by the GP flu vaccinations loss analysis database.
6. 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

7. The GP flu vaccinations loss analysis database is for use during the GP Flu Vaccinations Loss Analysis exercise, which aims to check and validate claims for payments and reimbursement made by GPs for providing seasonal flu vaccinations to eligible patients, with a view to producing some benchmark loss estimate figures in this area.

8. NHSCFA responsibility for the administration of the GP flu vaccinations loss analysis database is restricted to the loss analysis team.

9. Information in the GP flu vaccinations loss analysis database could include: flu vaccination record unique identifier; GP practice code; practice name and address; NHS England team; patient NHS number; patient name; patient address; patient date of birth; patient death status; patient date of death (if applicable); date flu vaccine administered; venue where flu vaccination took place; vaccine product used; name and professional registration number of the person who administered the vaccine; patient eligibility cohort group; item of service claim unique identifier; date item of service claim submitted; date item of service payment made; item of service payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the item of service claim; reimbursement claim unique identifier; date reimbursement claim submitted; name of vaccine product; date reimbursement payment made; reimbursement payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the reimbursement claim.

10. Sensitive data includes the patient's NHS number; patient name; patient address; patient date of birth; patient death status; patient date of death (if applicable); and clinical details of their flu vaccination treatment. This data is essential in order that they be checked and verified, in order to confirm the GP has submitted a legitimate claim for item of service fees and reimbursement of the vaccine. The data does not include any criminal offence information.

11. 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

12. The GP flu vaccinations loss analysis database is subject to the NHSCFA Data Handling and Storage Policy. Paper records are held by the Loss Analysis Team, part of the Strategic Intelligence Team of the Information and Intelligence Unit. All electronic and paper records are marked for deletion at the end of the data retention period, as specified in the NHSCFA Data Retention Schedule.

13. 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

14. The GP flu vaccinations loss analysis database is accessed by approximately 4 members of staff from NHSCFA and includes 2 database administrators

Section 5: External Sharing and Disclosure of Data

15. Information may be shared with other organisations such as NHSE&I, NHSBSA, DHSC, the Police, other law enforcement agencies, regulatory bodies, Local Counter Fraud Specialists, in accordance with NHCFA legal gateways. The only other reason information may be shared externally is to fulfil an FOI request, although data might only need to be displayed in a summary statistical format and presented in aggregate. No personal information will be shared.

Section 6: Notice/Signage

16. Data subjects are randomly selected for a loss analysis exercise and so are unlikely to be aware that we are processing their data until they are contacted to complete a questionnaire and as such will not have control of their data. Data subjects may not be informed that we hold information on them if it would prejudice law enforcement or the rights and freedoms of others.

17. 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.

18. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this Database and therefore outside the scope of this DPIA.

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

19. 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.

20. It is unlikely that many access requests will be received as the personal data recorded is all in relation to a GP flu vaccinations loss analysis exercise.

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

22. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

23. The security and technical access architecture of the GP flu vaccinations loss analysis database 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.

24. Access is restricted to internal staff only. 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.

    e. Secure access to folders when raw data is stored.

    f. Single point of entry to NHSCFA for workforce data.

Section 9: Technology

25. The GP flu vaccinations loss analysis database holds personal information obtained electronically and is located in the NHS Counter Fraud Authority data centre.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the GP flu vaccinations loss analysis database, 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 GP flu vaccinations loss analysis database 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. See also Annex A Category C.

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 GP flu vaccinations loss analysis database. 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 INFORMATION AND INTELLIGENCE UNIT
Project	GP Flu Vaccinations Loss Analysis exercise / database

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	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhscfa.gov.uk

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 GP flu vaccinations loss analysis database is required to help facilitate the GP Flu Vaccinations Loss Analysis exercise.

The database will store electronic data, relating to flu vaccinations administered to patients during the 2020-2021 flu season, extracted from a random sample of 200 GP practice systems. The data will be emailed to NHSCFA in password protected Microsoft Excel format using Egress secure file transfer. Once received, data will be copied or uploaded into a bespoke Microsoft Access database, which is the subject of this DPIA. The Access database and original Excel files will be held on a secure server. Additional supporting data will be supplied electronically by NHSE&I and NHSBSA, relating to claims for fees and reimbursements associated with the flu vaccinations. Other supporting information relating to the flu vaccinations will be provided by patients in hard copy format, by way of completed questionnaires returned to NHSCFA, which will be manually added to the project database.

Data could include: flu vaccination record unique identifier; GP practice code; practice name and address; NHS England team; patient NHS number; patient name; patient address; patient date of birth; patient death status; patient date of death (if applicable); date flu vaccine administered; venue where flu vaccination took place; vaccine product used; name and professional registration number of the person who administered the vaccine; patient eligibility cohort group; item of service claim unique identifier; date item of service claim submitted; date item of service payment made; item of service payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the item of service claim; reimbursement claim unique identifier; date reimbursement claim submitted; name of vaccine product; date reimbursement payment made; reimbursement payment amount; information on any errors, inaccuracies, corrections, withdrawals, overpayments and/or recoveries made in respect of the reimbursement claim.

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.

The GP flu vaccinations loss analysis database is for use during the GP Flu Vaccinations Loss Analysis exercise, which aims to check and validate claims for payments and reimbursement made by GPs for providing seasonal flu vaccinations to eligible patients, with a view to producing some benchmark loss estimate figures in this area. Regular loss analysis exercises are amongst the core functions of the NHS Counter Fraud Authority.

Losses can occur when a contractor wrongfully claims for an NHS service that was not provided, that cannot be substantiated, that did not comply with the rules on service provision or service specification, or that was not clinically needed, by way of false representation, by failing to disclose information and/or by abuse of position. Losses can also occur where the contractor makes a genuine mistake when claiming for a service.

The exercise will contact patients who, according to records submitted to NHS England and Improvement (NHSE&I) and/or NHS Business Services Authority (NHSBSA), received an NHS funded seasonal flu vaccination, and ask patients to confirm their experience of the service received. The exercise will also be checking and validating patient eligibility for an NHS funded seasonal flu vaccination with the relevant authorities.

This loss analysis exercise has been commissioned by the NHS Counter Fraud Board, comprising NHS Counter Fraud Authority, NHS England and Improvement, NHS Business Services Authority, Department of Health and Social Care and the Cabinet Office.

Access is restricted to 4 members of staff within NHSCFA, including 2 database administrators.

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 in the GP flu vaccinations loss analysis database has been 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 the GP flu vaccinations loss analysis database.

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.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH