NHS
Counter Fraud Authority

# Pharmacy Reward Scheme Database

## Privacy Impact Assessment

### November 2017

### V2.0 Published Version

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

# Executive summary

This document contains information in relation to the Pharmacy Reward Scheme (PRS) database.
The Pharmacy Reward Scheme allows pharmacists to claim a financial reward where they have identified a fraudulent prescription and either prevented fraud or contributed with valuable information to the investigation of Fraud. The fraudulent prescription would be a form which is not a genuine order for the person named on it, e.g. stolen or counterfeited and not signed by an authorised prescriber, or had been illegitimately altered by someone other than the authorised prescriber by whom it was issued. The reward is not payable for exemption fraud or for multi, or fraudulent, registration. It relates only to FP10 and not to private prescriptions.
The database contains the personal data of pharmacists who have made a claim to the scheme, individuals who have presented a fraudulent or counterfeit prescription and police officers to whom the fraud was reported and as such this document is deemed OFFICAL.

Any information viewed/obtained within this document should be treated in the appropriate manner as detailed in the terms and conditions of use for this site and as advised by the Government Security Classifications (2014).

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

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL and therefore there is no requirement to explicitly mark routine OFFICIAL information. However, any subset of OFFICIAL information which could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media 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, assets should be conspicuously marked: OFFICIAL–SENSITIVE'

# Table of contents

Table of contents ..... 3

Links & Dependencies ..... 5

Table 1 – Links and Dependencies ..... 5

Section 1: ..... 6

Privacy Impact Assessment Requirement & Process ..... 6

Introduction ..... 6

PIA Phases ..... 6

Pharmacy Reward Scheme  Database General Description ..... 7

Ownership ..... 8

Section 2: PIA Screening ..... 8

The PIA Screening Process ..... 8

Screening Process Conclusions ..... 14

Section 3: PIA Report ..... 15

Section 4: Compliance Checks ..... 21

DPA 98 Compliance Check ..... 21

The Privacy and Electronic Communications Regulations ..... 21

The Human Rights Act 1998 ..... 21

The Freedom of Information Act ..... 21

Annex A - Definition of Protected Personal Data ..... 22

Annex B – PRS Database Personal Data ..... 23

Annex C – Data Protection Compliance Check Sheet ..... 24

| Document Control | | | | | |
|---|---|---|---|---|---|
| **PM** | **Ref** | **Document owner** | **Version No** | **Issue Date** | **Amendments** |
| **Information and Records Management Officer** | **PIA/PRS Database** | **DPO** | **V0.1** | **09/11/2017** | **All** |
| **Information and Records Management Officer** | **PIA/PRS Database** | **DPO** | **V0.2** | **20/11/2017** | **Comment from TD** |
| **Information and Records Management Officer** | **PIA/PRS Database** | **DPO** | **V1.0** | **07/03/2019** | **Redacted for publication** |
| **Information and Records Management Officer** | **PIA/PRS Database** | **DPO** | **V2.0** | **13/09/2021** | **Reviewed and anonymised for final publication – no amendments to original version completed in 2017** |

| Prefix | |
|---|---|
| **Reference:** | **PIA/PRS Database** |
| **Date:** | **November 2017 (Original completion date)** |
| **Author:** | **Information and Records Management Officer** |
| **Data Owner:** | **Information Systems and Analytics Manager** |
| **Version:** | **2.0** |
| **Supersedes** | **1.0** |

## Links & Dependencies

| Document | Title | Reference | Date | POC |
|---|---|---|---|---|
| DPA | Data Protection Act | All | 1998 | 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 | April 2014 | 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<br>P2 – Issue 3.5 | October 2009<br>October 2009 | CESG |
| IS2 | InfoSec Standard 2 | Issue 3.2 | January 2010 | CESG |
| PECR | The Privacy and Electronic Communications Regulations | All | 2003 | HMG |

**Table 1 – Links and Dependencies**

# Section 1:

# Privacy Impact Assessment Requirement & Process

## Introduction

1. Although the Information Commissioner's Office ("ICO") has not decreed that there is a legal obligation to undertake a Privacy Impact Assessment ("PIA") on systems holding personal or private data, all HMG departments are being mandated to conduct an assessment. NHS Protect (whose fraud functions have now been transferred to and taken over by NHSCFA) has agreed that all systems that process or store personal data on more than 250 people will require a PIA to be conducted and documented as part of the accreditation evidence.

2. A PIA is defined as a process whereby the potential privacy impacts of a project are identified and examined from the perspectives of all stakeholders in order to find ways to minimise or avoid them. It enables organisations to anticipate and address the potential privacy impacts of new initiatives or systems. The identified risks to an individual's privacy can be managed through consultation with key stakeholders and where applicable systems can be designed to avoid unnecessary privacy intrusion.

3. Ideally, PIAs should be undertaken at the beginning of the project's life cycle so that any necessary measures and design features are built in; this minimises the risk to the project both in terms of ensuring legal compliance and addition of costly retrospective security controls.

4. This PIA is related to the NHS PROTECT RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS was developed in accordance with the requirements of NHS Protect and CESG HMG Infosec Standards 1 and 2.

## PIA Phases

5. The ICO PIA Handbook suggests 5 phases to a PIA:

a. Preliminary Phase – This phase establishes the scope of the PIA, how it is going to be approached and identifies tasks, resources and constraints.

b. Preparatory Phase – This phase organises and makes arrangements for the next phase of the process; the Consultation and Stakeholder analysis;

c. Consultation and Analysis Phase – This phase focuses on consultation with the system stakeholders (including clients/customer where applicable), risk analysis with respect to privacy, recognition of privacy issues and identification of potential solutions;

d. Documentation Phase – This phase documents the results of the Consultation and Analysis Phase to include a summary of issues and proposed actions, where required;

e. Review and Audit Phase – The review and audit process is maintained until the system or application is decommissioned and disposed of. Reviews and audits should be conducted annually or at times of significant change to ensure that there is no change of impact or risk with respect to privacy.

## Pharmacy Reward Scheme Database General Description

6. The Pharmacy Reward Scheme was introduced in 1999 to allow pharmacists to claim a financial reward where they have identified a fraudulent prescription and either prevented fraud or contributed with valuable information to the investigation of Fraud.
   The fraudulent prescription would be a form which is not a genuine order for the person named on it, e.g. stolen or counterfeited and not signed by an authorised prescriber, or had been illegitimately altered by someone other than the authorised prescriber by whom it was issued. The reward is not payable for exemption fraud or for multi, or fraudulent, registration. It relates only to FP10 and not to private prescriptions. The scheme consists of a database and a manual filing system containing paper claim forms and correspondence.

7. The Pharmacy Reward is payable where:
   - ❖ Fraudulent activity can be proven, and
   - ❖ Conditions of the scheme are met.

   There are two elements to the reward, the Retention and the Reporting Reward.
   The Reward has been set at a flat rate of £70.00 to compensate pharmacists adequately for their efforts in reporting incidents where fraud has taken place, and contributing valuably to the work of countering fraud and corruption within the NHS.

   **Retention Reward**
   If the pharmacist has not dispensed or part dispensed the drugs, medicines or listed appliances, and has retained the prescription, they may claim the retention element of the reward if they meet the criteria.
   **Reporting Reward**
   If the pharmacist has dispensed the drugs, medicines or listed appliances, but had reason to believe at the time, or subsequently comes to have reason to believe that the prescription is not genuine they can claim for the reporting element of the reward
   if they meet the criteria.

8. The process involves the pharmacist contacting NHSCFA Service Desk by telephone within seven days to report that a fraudulent prescription has been presented, before completing a form posted out by Service Desk with a covering letter and returning it within 28 days in order to claim the reward.
   The circumstances of the claim are examined and a decision made as to whether the reward is payable.

9. Service Desk are responsible for the administration of the scheme, and populate the database manually from receipt of the initial telephone call when the claim in registered, and then on receipt of the completed claim form. At the time of writing there are 4804 claim records in the database.

10. For security and confidentiality purposes, the database is only accessed by approximately 10 members of staff from NHSCFA, which includes the database administrators.

11. This is the only Privacy Impact Assessment to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with the Information Governance and Risk Management Lead.

12. The Pharmacy Reward Scheme Database, is required to comply with relevant HMG legislation including where applicable the Data Protection Act 1998, Human Rights Act 1998 and Freedom of Information Act 2000. To ensure that it meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a PIA which is broken down into the following stages:

    a. PIA Screening. (This is a condensed screening process using the Pre Privacy Impact Assessment Questionnaire adapted by NHS Protect (Now NHSCFA). The output will determine if a PIA is required and indicate how much effort is required depending on the type, quantity and sensitivity of the personal information involved).

    b. PIA Assessment and Report;

    c. Compliance Checks;

    d. Summary and Conclusions

## Ownership

13. The following tables describes the Pharmacy Reward Scheme Database roles and responsibilities:

| Role | Responsibility |
|---|---|
| Information Asset Owner (IAO) | Information Systems and Analytics Manager |
| Senior Responsible Officer (SRO) | Head of Intelligence and Fraud Prevention |
| Application Owner | Information Systems Lead |
| Data Protection Officer | Information Governance and Risk Management Lead |

# Section 2: PIA Screening

## The PIA Screening Process

1. The initial PIA screening process determines if a PIA is required to be conducted. The decision is based on the quantity and sensitivity of the personal data being processed and any privacy impacts. The categorisation of sensitive personal data is described in Annex A.

2. The screening process has used the Pre Privacy Assessment Questionnaire originally created by NHS Protect and whose fraud functions have now transferred to NHSCFA, to determine whether a PIA is required. The intention of the questionnaire is not to provide over elaborate answers but to demonstrate that all aspects of the project have been considered regarding personal data. Once completed, the IAO and DPO are required to assess the responses to determine if a PIA needs to be conducted. The responses provided in the Pre PIA Questionnaire and DPO/IAO decision are to be made available to the Accreditor.

3. **The ICO PIA template notes that organisations can choose to adapt the process and the PIA template to produce something that allows them to conduct effective PIAs integrated with the project management processes and fits more closely with the types of project likely to be assessed. Therefore, this is a questionnaire adapted specifically for NHS Protect, subsequently used by NHSCFA and slightly differs from the ICO screening questionnaire, whilst covering the same issues and content.**

| Ser | Question | Response |
|---|---|---|
| **1** | System/Application/Project Name | Pharmacy Reward Scheme Database |
| **2** | What is the main function of the System/Application/Project? | The main function of the database is to administer a process that allows pharmacists to claim a financial reward where they have identified a fraudulent prescription and either prevented fraud or contributed with valuable information to the investigation of Fraud.<br><br>There are two elements of the reward namely:- reporting or retention and either one is payable at £70 depending on the circumstances surrounding the claim.<br><br>The process involves the pharmacist contacting NHSCFA Service Desk by telephone within seven days to report that a fraudulent prescription has been presented, before completing a form sent out by Service Desk with a covering letter, and returning within 28 days in order to claim the reward. The circumstances of the claim are examined and a decision made as to whether the reward is payable.<br><br>Service Desk are responsible for the administration of the scheme, and populate the database manually from receipt of the initial telephone call when the claim in registered, and then on receipt of the completed claim form. At the time of writing there are 4804 claim records in the database, and the unique PRS claim number is automatically generated when a new claim is added. |
| **3** | Briefly, what are the personal data elements used by the System/Application/Project? See Annex A for guidance, | Information that can be used to identify a living person |

| | | |
|---|---|---|
| **4** | What [1]personal data is collected? (See Annex A for definitions) | The database contains the following information:<br>Name of pharmacist / person(s) claiming the reward. (Home address if Locum Pharmacist)<br>Business name, address, tel no and fax no of pharmacy where prescription presented.<br>Unique contractor account number serial number of prescription, date/ time presented, patients name(possibly fictitious) gender and description, medications prescribed, circumstances surrounding the claim and any vehicle details , Name and collar number of police officer dealing, address of police station, date reported and crime reference.<br>Sensitive Data as listed in Annex A of PIA would be: Alleged commission of offences for individual presenting the fraudulent prescription. |
| **5** | From who is the personal data collected? | The personal data is collected from the pharmacist making the claim to the Pharmacy Reward Scheme, and collated from the initial telephone call, the completed claim form and also the prescription. |
| **6** | Why is the personal data being collected? | The data is collected to enable the Pharmacy Reward Scheme to be administered and also for evidence of a fraudulent prescription being presented, in order to validate the reward payment. |
| **7** | How is the personal data collected? | Information is collected from the pharmacist during the initial telephone call where details of the claim are taken and the claim form posted out.<br>Further data is copied to the database from the completed claim form and prescription once returned and also from any follow up calls with the pharmacist or the police. |
| **8** | Describe all the uses for the personal data (including for test purposes). | Data in respect of the pharmacist is required as a mechanism of communicating with them in the administration of the scheme and in order for payments to be made.<br>Data in respect of the patient / person presenting the fraudulent prescription is used for the administration of justice.<br>Data in respect of the police would be Business Card Information only.<br>Data is not used for test purposes. |

[1] Note the DEPT Chief Information Officers Department has confirmed that 'Business card' information should not be classed as personal information. Business Card Information includes: Name, Post/Role, Work Address and Contact details.

| | | |
|---|---|---|
| **9** | Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern? | The system doesn't currently analyse the personal data, however the database had been designed so that analysis can be undertaken if required. |
| **10** | Is the personal data shared within internal organisations? | Access is restricted to approximately ten members of staff within NHSCFA including the database administrators. |
| **11** | For each organisation, what personal data is shared and for what purpose? | Access is restricted to approximately ten members of staff within NHSCFA including the database administrators. The data is not shared as such but staff have access to the information within the database and also the corresponding claim forms |
| **12** | Is personal data shared with external organisations? (If No go to Q15) | Information would only be shared with the police if it was requested for the administration of justice. |
| **13** | Is personal data shared with external organisations that are not within the [2]European Economic Area? | No |
| **14** | For each external organisation, what personal data is shared and for what purpose? | Information would only be shared with the police if it was requested for the administration of justice. The Business Services Authority (BSA) are responsible for making all payments to pharmacists by way of a payment schedule from their contractor payments team , and as such, the closure form containing details of the pharmacy and contractor account number would be shared with them to facilitate the reward payment. |
| **15** | How is the personal data transmitted or disclosed to internal and external organisations? | Information would normally be shared with the police via telephone should they require it.<br>The closure form to the BSA containing the Pharmacy address and unique contractor account number would be sent via internal post. |
| **16** | How is the shared personal data secured by the recipient? | Information shared with the police would be secure and the information shared with the BSA is in respect of the pharmacy name, address and contractor number which would be classed as business card information. |

[2] Norway, Iceland and Lichtenstein together with other European Union Nations and Switzerland make up the European Economic Area.

| | | |
|---|---|---|
| **17** | Which User group(s) will have access to the system? | Access is restricted to staff from NHSCFA Service Desk.<br><br>System Administrators will also have access. |
| **18** | Will contractors/service providers to NHS Protect have access to the system? | No |
| **19** | Does the system use “roles” to assign privileges to users of the system? | Yes, only specific users have the required permissions to access the system. |
| **20** | How are the actual assignments of roles and rules verified according to established security and auditing procedures? | Access is restricted to staff from NHSCFA Service Desk.<br><br>System administrators also have full access to all data. |
| **21** | What is the current accreditation of the system? | Official (Sensitive) |

**Table 2 - PIA Screening Questionnaire**

4. Having completed the questions in the table above it should be possible to confirm what type of personal data is being processed by the system/application and whether a PIA is required and the type and level of detail required. Essentially if any of the responses to questions 1-3 is yes then a PIA is required. The following questions are mandatory and must be completed:

| Ser | Question | Response |
|---|---|---|
| 1 | Will personal data be processed, stored or transmitted by the system/application? (If No go to Q4) | Yes |
| 2 | Will the project process, store or transmit more than 250 Personal Data records (If No go to Q3) | Yes |
| 3 | Will [3]sensitive personal data be processed, stored or transmitted by the system/application? | Yes |
| 4 | Is a PIA required for the system / application? (If No go to signature block) | Yes |
| 5 | What level of scale of PIA is required? (Guidance should be sought from the DPO, IAO and Accreditor) | Full |

**Table 3 – PIA Decision Criteria**

[3] Sensitive personal data is personal data that consists of racial or ethnic origin, political opinions, religious beliefs etc – full details of sensitive personal data is available in the Data Protection Act 1998, see Annex A.

## Screening Process Conclusions

5. The screening process, completed in November 2017, identified the following PIA requirements of using the Pharmacy Reward Scheme (PRS) Database.

a. Although not undertaken at the beginning of the project, a Privacy Impact Assessment (PIA) is required.

b. The PIA should after consultation with the DPO, IAO and Accreditor be completed in accordance with the adapted PIA template which is based on the full scale assessment. The requirements from which this template was derived are described on the ICO website at https://ico.org.uk/media/for-organisations/documents/1042836/pia-code-of-practice-editable-annexes.docx

c. The following legal requirements apply to the system and in addition to this there is also a Risk Assessment report available.

i. Data Protection Act 1998

ii. Human Rights Act 1998

iii. Freedom of Information Act 2000

6. The conclusion reached following the review of this screening is that,

a. There is great benefit to having a documented list of the considerations related to the processing of personal data within the PRS Database, including the purposes for which it is gathered and outputs it produces.

b. This benefit is increased further when it is considered that some elements of the data capture are potentially contentious (i.e. personal data in relation to subjects), and that documented evidence of the considerations surrounding them and justifications for use is additionally of benefit and can provide assurance.

# Section 3: PIA Report

## Data Collection and Maintenance

1. The Pharmacy Reward Scheme is administered by way of a database and a manual filing system. The database was created in 2003 to electronically record details of claims to the scheme. The scheme itself which was originally introduced in 1999, allows pharmacists to claim a financial reward where they have identified a fraudulent prescription and either prevented fraud or contributed with valuable information to the investigation of Fraud.

2. The database contains the following information: Name of pharmacist / person(s) claiming the reward Business name, address, tel no and fax no of pharmacy where prescription presented. (Home address if Locum Pharmacist) Unique contractor account number serial number of prescription, date/ time presented, patients name(possibly fictitious) address, dob, gender and description, medications prescribed, circumstances surrounding the claim and any vehicle details , Name and collar number of police officer dealing, address of police station, date reported and crime reference. Also included is sensitive data as listed in Annex A of the PIA:
Alleged commission of offences for individual presenting the fraudulent prescription

3. The impact level of the PRS Database was assessed as CONFIDENTIAL and it can only be accessed internally.

4. The following measures briefly describe what controls have been implemented to protect the PRS Database and the personal data recorded:

   a. All off site back-ups are secure as they can only be opened via the encryption key.

   b. The PRS Database is only accessed by approximately 10 members of staff from NHSCFA, which includes the database administrators

   c. The PRS Database does not have any direct interconnections with other NHSCFA systems and applications.

   d. 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 Pharmacy Reward Scheme Database. Risks to confidentiality are listed in the Risk table below.

6. This PIA 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.

7. The privacy risks and associated mitigations are described in Table 4. The IAO is responsible for mitigating the risk.

| Risk Description | Mitigation |
|---|---|
| 1. There is a risk that the personal data is used for other purposes than for what it was originally intended for. | The data is processed to enable the Pharmacy Reward Scheme to be administered and to determine if the claim meets the criteria for payment.<br>It would not be used for any other purpose. |
| 2. There is a risk that excessive personal data is collected on an individual. | This PIA exists to ensure that there is due consideration as to the extent of the data used. |
| 3. There is a risk that personal data is retained for longer than necessary. | The Pharmacy Reward Scheme is subject to NHSCFA Data Handling and Storage Policy<br>However, there is currently no deletion process in place and as such there are details of claims dating back to 2003 recorded in the database.<br>The claim forms and respective correspondence are stored in a locked filing cabinet before being sent to the warehouse where they are retained for 7 years prior to being destroyed. |
| 4. There is a risk that the personal data is no longer relevant. | Data recorded in the Pharmacy Reward Scheme database, relates either to individuals who have reported that a fraudulent prescription has been presented, been the subject to have presented the fraudulent prescription or the police officer who has dealt with the case.<br>The data would be relevant as it is evidence of fraudulent behaviour. It can be analysed for patterns or trends and to check if the person presenting the fraudulent prescription has done so previously. |
| 5. There is a risk that the personal data is not accurate or up to date. | The information in the claim form has been provided voluntarily by the pharmacist.<br>The information from both the claim form and the prescription in respect of the patient / person presenting the prescription or information in the claim form in relation to the police officer dealing with the case, is copied manually to the PRS database by NHSCFA Service Desk and as this is a manual process, they would be responsible for the accuracy of the data.<br>NHSCFA has no means to audit or review this data for accuracy. |

| | |
|---|---|
| 6. There is a risk that the confidentiality of the personal data is not adequately protected. | All risks in relation to security and other protective measures have been identified and all risks relating to confidentiality have been mitigated as far as possible. |
| 7. There is a risk that personal data is passed to external organisations. | The only information shared with external organisations, would be with the police if it was requested for the administration of justice, and with the BSA to facilitate the reward payment to the contractor. |
| 8. There is a risk that personal data is hosted or exported outside of the EU. | No data will be exported outside the UK |

**Table 4 – Privacy Risks**

## Section 2: Uses of the Application and the Data

8. The Pharmacy Reward Scheme database is used to record claims when a fraudulent, stolen or counterfeit prescription has been presented. The process involves the pharmacist contacting NHSCFA Service Desk by telephone within seven days to report that a fraudulent prescription has been presented, before completing a pre numbered form issued by Service Desk, and returning within 28 days in order to claim the reward.
   The circumstances of the claim are examined and a decision made as to whether the reward is payable.

9. Service Desk are responsible for the administration of the scheme, and populate the database manually from receipt of the initial telephone call when the claim in registered, and then on receipt of the completed claim form. At the time of writing there are 4804 claim records in the database, and the unique PRS claim number is automatically generated when a new claim is added.

10. Written correspondence is sent to the pharmacist, to confirm if the reward will be paid or if the claim did not meet the criteria. Written or email correspondence is sent to the officer in charge of the case. A closure form outlining the reward to be paid is sent to the BSA in order to facilitate the payment.

11. Information in the database could include Name of pharmacist / person(s) claiming the reward Business name, address, tel no and fax no of pharmacy where prescription presented. (Home address if Locum Pharmacist) Unique contractor account number serial number of prescription, date/ time presented, patients name(possibly fictitious) address, dob, gender and description, medications prescribed, circumstances surrounding the claim and any vehicle details , Name and collar number of police officer dealing with the case, address of police station, date reported and crime reference.

12. Also included is sensitive data as listed in:
    Annex A of the PIA: Alleged commission of offences for individual presenting the fraudulent prescription.

13. The measures that have been implemented to protect the Personal Data are:

    a. Access is restricted to approximately ten members of staff within NHSCFA including the database administrators.

    b. The Pharmacy Reward Scheme database does not have a direct interconnection with other NHSCFA systems or applications.

    c. 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

14. The Pharmacy Reward Scheme is subject to NHSCFA Data Handling and Storage Policy
    However, there is currently no deletion process in place and as such there are details of claims dating back to 2003 recorded in the database.

    The claim forms and respective correspondence are stored in a locked filing cabinet before being sent to the warehouse where they are retained for 7 years prior to being destroyed.

15. . The IAO is required to review the retention period and any requirement to change must be submitted to the Application Change Board.

## Section 4: Internal Sharing and Disclosure of Data

16. Access is restricted to approximately ten members of staff within NHSCFA including the database administrators.

## Section 5: External Sharing and Disclosure of Data

17. The only information shared with external organisations, would be with the police if it was requested for the administration of justice, and the closure form with the BSA to facilitate the reward payment.

## Section 6: Notice/Signage

18. Pharmacists are aware of the data that we hold for them as they have provided it both over the telephone whilst registering the claim and also within the completed claim form. We also liaise with the police officer to whom the case was assigned to so they are aware that we hold business card information for them. It would not be reasonable to notify the patient/individual presenting the fraudulent prescription as this may include an allegation of fraud and be subject of an investigation.
19. NHSCFA hosts a subsection within their website entitled “How we handle information” within which there are 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.
20. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to the Pharmacy Reward Scheme Database and therefore outside the scope of this PIA.

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

21. Individuals 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, except where the usual exemptions may apply.
22. It is unlikely that many access requests will be received as the personal data recorded is all in relation to the presentation of fraudulent prescriptions which may result in an investigation, and as such are confidential until such point they are substantiated
23. In the unlikely event that that information is identified as being incorrect, NHSCFA Service Desk correct the record.
24. 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

25. The security and technical access architecture of the PRS Database is as explained in this PIA:

    The application and the hosting infrastructure was assessed at Official Sensitive and the hosting infrastructure is subject to CESG approved IT Security Health Check.

26. Access is restricted to internal staff only.

27. 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

28. The Pharmacy Reward Scheme Database holds personal information taken both by telephone and from completed claim forms and is located in the NHS Counter Fraud Authority data centre.

## Conclusion

29. There are no residual privacy risks to the personal data recorded in the Pharmacy Reward Scheme Database. The controls described in this PIA explain in detail how the data is protected and managed in accordance with the DPA98. The DPO is responsible for ensuring that the controls are implemented through the lifecycle of the system.

# Section 4: Compliance Checks

## DPA 98 Compliance Check

1. The DPO must ensure that the Pharmacy Reward Scheme Database, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

   a. 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 application process sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of DPA98 have been complied with, see Annex 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 public authority we are compliant with the provisions of the Freedom of Information Act, in publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, there would be no personal information disclosed under the Freedom of Information Act as this would breach the data protection principles.

# 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 Data Protection Act 1998 (DPA98).

Particular care must be taken with data in Category B and with any large data set (i.e. consisting of more than 250 records). 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 in DPA98 on the processing of data in Category C.

## Annex B – Pharmacy Reward Scheme Database Personal Data

1. The table below lists and describes all the personal data processed and stored in the system. It also includes a justification of the requirement for its use.

| No | Personal Data | Justification |
|---|---|---|
| 1 | For Pharmacist:<br><br>Name, business address, telephone and fax numbers<br><br>Unique contractor account number.<br><br>Home address for locum pharmacist | To allow for channels of communication and facilitate the payment of the reward.<br><br>To facilitate the reward payment.<br><br>To enable communication to home address when the pharmacist rotates to different pharmacies. |
| 2 | For Police Officer:<br><br>Name and collar number<br><br>Business address /station | For the administration of justice to investigate the presentation of fraudulent prescriptions. |
| 3 | For Patient / Individual presenting the prescription:<br><br>Patients name (possibly fictitious)<br><br>Address and dob<br><br>Gender and description.<br><br>Prescribed medications<br><br>Possible vehicle details<br><br>Alleged commission of offences: i.e presentation of fraudulent / stolen or counterfeit prescription. | For the administration of justice |

# Annex C – 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 | Pharmacy Reward Scheme 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 PIA)

| | |
|---|---|
| Name, Title | Trevor Duplessis |
| Branch / Division | Finance and Corporate Governance, NHSCFA |
| Phone Number | 020 7895 4642 |
| E-Mail | Trevor.Duplessis@nhscfa.gsi.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 Pharmacy Reward Scheme Database was created in 2003 to electronically record details of claims to the scheme. The scheme itself which was originally introduced in 1999, allows pharmacists to claim a financial reward where they have identified a fraudulent prescription and either prevented fraud or contributed with valuable information to the investigation of Fraud.

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

NHSCFA leads on a wide range of work to protect NHS staff and resources from crime.

The purpose of the Pharmacy Reward Scheme, which consists of a database and a paper based filing system, is to facilitate the processing of claims and payment of rewards in respect of the scheme, in addition to recording information in relation to individuals responsible for presenting fraudulent stolen or counterfeit prescriptions.

Access is restricted to ten members of staff within NHSCFA, including the database administrators.

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

| |
|---|
| Privacy impact assessments have been considered in the light of personal data gathered, and the data in the Pharmacy Reward Scheme 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 4 of this document) |

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

| |
|---|
| This is the first PIA carried out on the system. |

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

| |
|---|
| *IMPORTANT NOTE:<br>'Personal data' means data which relate to a living individual who can be identified:<br>(a) from those data, or<br><br>(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,<br><br>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.<br><br>(Data Protection Act, section 1) |

## NHSCFA offices

**Coventry**

Cheylesmore House
5 Quinton Road
Coventry
West Midlands
CV1 2WT

**London**

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

**Newcastle**

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH