NHS
Counter Fraud Authority

Health and Social Care Act Database

Privacy Impact Assessment

November 2017

V1.0

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

Executive summary

This document contains information in relation to a Health and Social Care (HSCA) database, comprising of personal data of individuals who have been the subject of an Advance Warning. Advance Warnings contain information regarding forthcoming trials and are issued where it is anticipated that an NHS fraud investigation has the possibility of generating external interest. The database was created in 2012 to be used as a checking mechanism, for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA through NHS Protect, whose fraud functions from 1st November 2017 have been transferred to NHSCFA, to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for fraud. As such the 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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Susan Hyde	PIA / HCSA Database	Trevor Duplessis	V0.1	02/11/2017	All
Susan Hyde	PIA / HCSA Database	Trevor Duplessis	V0.2	09/11/2017	Amendments from TD
Susan Hyde	PIA / HCSA Database	Trevor Duplessis	V0.2	07/03/2019	Redacted for Publication

Prefix	
Reference:	**PIA/HSCA Database**
Date:	**November 2017**
Author:	**Susan Hyde**
Data Owner:	**Gillian Dalton**
Version:	**1.0**
Supersedes	**0.2**

Links & Dependencies

Document	Title	Reference	Date	POC
Government Security Classifications	Government Security Classifications	All	April 2014	Cabinet Office
EU GDPR	EU General Data Protection Regulation	All	May 2018	GDPR
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
DPA	Data Protection Act	All	1998	HMG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG
HRA	Human Rights Act	All	1998	HMG
FOI	Freedom of Information Act	All	2000	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.

Health and Social Care Act Database General Description

6. The Health and Social Care Act (HSCA) Database contains personal data of individuals who have been the subject of an Advance Warning. The warnings contain information regarding forthcoming fraud trials and are issued by external Local Counter Fraud Specialists based at NHS organisations or Senior Fraud Investigators from NHS Counter Fraud Authority (NHSCFA) where it is anticipated that an NHS fraud investigation has the possibility of generating external interest.

7. The HSCA Database was created in 2012 for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA(Business Services Authority) through NHS Protect (now NHSCFA) to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for fraud. The regulations state that when a performer wishes to apply to be on a performers list within a specific area team in NHS England, they have to apply to the individual employing authority, who in turn must ask NHS Protect (now NHSCFA) to undertake a check to determine if the applicant has ever been subject to a fraud investigation.

8. The process includes the use of a dedicated HSCA mailbox for the receipt of the Advance Warning and also for receiving and responding to requests for checks to be conducted.

9. Although the content of the Advance Warning contains both personal and sensitive information, the only information transferred to the actual database would be the name, date of birth, professional registration number and occupation.

10. Service Desk receive the Advance Warning via the shared HSCA mailbox, and they manually update the HSCA database using details from the Advance Warning. This is the only information used to populate the database.

11. Service Desk also receive requests in to the HSCA mailbox to check if a performer has ever been investigated for fraud. They may also receive requests to check if there are any adverse records held on a corporate body; however these are forwarded for a separate check in iBase as there is no facility to check corporate bodies in the HSCA database.

12. There are on average approximately 500 HSCA checks requested each month with only 2% having a positive result. As such, the mailbox holds the personal details of individuals who have not been subject of a fraud investigation.

13. The requests are from NHS England and occasionally from Scotland or Wales where the performer (contractor) was previously registered in England. When there is no fraud matched to the person's name and date of birth, the results of the check are shared by Service Desk with the requester, however where there is found to be a positive match, the information is forwarded to the Information Governance Officer to be investigated further using iBase and for a separate response.

14. The mailbox used in conjunction with the database holds results of checks and details of advance warnings, going back historically in the archive to 2003.

15. For security and confidentiality purposes, the database is only accessed by Five members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist

16. 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.

17. The HSCA 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

18. The following tables describes the HSCA Database roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Gillian Dalton
Senior Responsible Officer (SRO)	Richard Hampton
Application Owner	Richard Hampton
Data Protection Officer	Trevor Duplessis

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 NHSProtect Pre Privacy Assessment Questionnaire 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 NHSProtect specific questionnaire and slightly differs from the ICO screening questionnaire, whilst covering the same issues and content.**

Ser	Question	Response
1	System/Application/Project Name	HSCA Database
2	What is the main function of the System/Application/Project?	The main function of the database is to undertake employment checks on contractors who are applying for positions within the NHS. The database contains personal data of individuals who have been the subject of an Advance Warning. The warnings contain information regarding forthcoming fraud trials and are issued by external Local Counter Fraud Specialists based at NHS organisations or Senior Fraud Investigators from NHS Counter Fraud Authority (NHSCFA) where it is anticipated that an NHS fraud investigation has the possibility of generating external interest. The HSCA Database was created in 2012 for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for fraud. The regulations state that when a performer wishes to apply to be on a performers list within a specific area team in NHS England, they have to apply to the individual employing authority, who in turn must ask NHSCFA to undertake a check to determine if the applicant has ever been subject to a fraud investigation. The process includes the use of a dedicated HSCA mailbox for the receipt of the Advance Warning and also for receiving and responding to requests for checks to be conducted. Although the content of the Advance Warning contains both personal and sensitive information, the only information transferred to the actual database would be the name, date of birth, professional registration number and occupation. The system is reliant on LCFSs informing NHSCFA of a fraud investigation by way of an Advance Warning. Checks can only be undertaken against information provided to us; therefore there may be an occasion when an individual has been subject to a fraud investigation, but because we have not been provided with an AW, it would result in an incorrect search finding being communicated to the employing authority.

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 is reliant on information gathered from Advance Warnings and although there is a lot of data in the AW, the only information transferred to the database is: name, date of birth, professional registration number and occupation. Additional information contained in the Advance Warning itself and retained in the HSCA mailbox might include the address, Sensitive Data as listed in Annex A of PIA *Commission or alleged commission of offences for Subjects. *Proceedings relating to an actual or alleged offence for Subjects. *Racial or ethnic origin of Subject In addition to this, there will also be personal information in the mailbox regarding contractors who have applied for a position within the NHS and for which a check is necessary, but who have not been the subject of an NHS investigation.
5	From who is the personal data collected?	The personal data in the database is transferred from the Advance Warnings. The information in the Advance Warnings is provided by external Local Counter Fraud Specialists based at NHS organisations as well as Senior Fraud Investigators from NHSCFS. Additionally, information is contained in the mailbox where a check is requested for a contractor, and includes individuals who have never been the subject of a fraud investigation.
6	Why is the personal data being collected?	The data is collected as a mechanism to check if a health professional applying to be on the contractors list in a specific area, has ever been investigated for fraud.

[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.

7	How is the personal data collected?	Information is copied to the database manually from the Advance Warnings.
8	Describe all the uses for the personal data (including for test purposes).	The data is used to check if a health professional applying to be on the contractors list in a specific area, has ever been investigated for fraud. Data is not used for test purposes.
9	Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern?	The system does not analyse the personal data as such, however the database can be filtered to search for specific information. The database is made up of a search page where the search criteria is inputted, and a spreadsheet of data behind from where the results are extracted.
10	Is the personal data shared within internal organisations?	Access is restricted to four members of staff from the NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist
11	For each organisation, what personal data is shared and for what purpose?	Access is restricted to four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist
12	Is personal data shared with external organisations? (If No go to Q15)	Results of checks where there is a positive match to an individual having been investigated for fraud are shared with the employing authority who has requested the check.
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?	Written in to the National Health Service (Performers Lists) (England) Regulations 2013 is the obligation for NHSCFA (previously NHS Protect) to check and provide the results of any positive matches to the employing authority of any health professional who has ever been investigated for fraud. As such, positive matches are shared with the employing authority.
15	How is the personal data transmitted or disclosed to internal and external organisations?	The data would be transmitted via a confidential email account where access to the mailbox is restricted.

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

16	How is the shared personal data secured by the recipient?	The HSCA database is not designed to be accessed externally, however results of checks where there is a positive match, would be emailed securely to the recipient who have their own secure systems.
17	Which User group(s) will have access to the system?	Access is restricted to four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist System Administrators will also have access.
18	Will contractors/service providers 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 four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist 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 However this is recorded in the Advance Warning stored in the mailbox only, and would not be processed in the actual database.
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 HSCA 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 http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/26-report.html

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 HSCA 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 HSCA Database is a system created in 2012 for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for fraud. As such, the HSCA Database holds personal data of individuals who have ever been the subject of an NHS fraud investigation, and is reliant on information contained in Advance Warnings (AW) Also contained in the database is a snapshot of data taken from the Case Management System when the database was created and prior to the information from Advance Warnings being added.

2. Advance Warnings (AW's) are linked to investigations and contain information regarding forthcoming trials, and although there is a lot of data in the AW, the only information transferred to the database is: name, date of birth, professional registration number and occupation.

3. Additional information contained in the Advance Warning itself and retained in the HSCA mailbox might include:
   Address,
   Sensitive Data as listed in Annex A of PIA
   *Commission or alleged commission of offences for Subjects.
   *Proceedings relating to an actual or alleged offence for Subjects.
   *Racial or ethnic origin of Subject
   In addition to this, there will also be personal information in the mailbox regarding contractors who have applied for a position within the NHS and for which a check is necessary, but who have not been the subject of an NHS investigation.

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

5. The following measures briefly describe what controls have been implemented to protect the HSCA 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 HSCA Database will only be accessed by four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist.

   c. The HSCA Database does not have any direct interconnections with other NHSCFA systems and applications. However the information held within it has all originated from the Advance Warnings.

   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 NHSProtect register and the NHSCFA DPO is aware of its existence.

6. It is assessed that there are no residual privacy risks to the personal data used by the HSCA Database. Risks to confidentiality are listed in the Risk table below.

7. 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.

8. 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 as a checking mechanism for NHS employing authorities. 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 HSCA Database is subject to NHSCFA Data Handling and Storage Policy and will be audited annually to ensure that personal data is not retained longer than necessary.
4. There is a risk that the personal data is no longer relevant.	Data recorded in the HSCA Database, relates to individuals who have **EVER** been subject to an Advance Warning in respect of NHS Fraud, and as the database was designed with this in mind, there are no entry dates and no way of determining how long a record has been there, if it is still relevant or if it is out of date.
5. There is a risk that the personal data is not accurate or up to date.	Information is provided in Advance Warnings by individual NHS organisations from their own systems or the Senior Fraud investigator from NHSCFA. Lead Investigators of each case would be responsible for the accuracy of gathered data, for both their own records and additionally for information provided to us. Staff from NHSCFA Service Desk, manually copy the personal data from the Advance Warning in to the HSCA Database. NHSCFA has no means to audit or review this data for accuracy. It is appropriate to add that, The system is reliant on LCFSs informing NHSCFA of a fraud investigation by way of an Advance Warning. Checks can only be undertaken against information provided to us; therefore there may be an occasion when an individual has been subject to a fraud investigation, but because we have not been provided with an AW, it would result in an incorrect search finding being communicated to the employing authority
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 passed to external organisations, would be if there was a positive result to a check undertaken on behalf of an NHS organisation. The result would be shared with the employing authority.
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

9. The HSCA Database is a database and confidential email system containing personal information in relation to individuals who have EVER been the subject of an NHS fraud investigation.

The database was created in 2012 for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for fraud.
A separate check is also undertaken for Corporate Bodies; i.e Pharmacies, however these are checked in a system called iBase and not from the HSCA database.
The regulations state that when a performer wishes to apply to be on a performers list within a specific area team in NHS England, they have to apply to the individual employing authority, who in turn must ask NHSCFA to undertake a check to determine if the applicant (or in the case of a pharmacy – the Corporate Body) has ever been subject to a fraud investigation.
The HSCA database was initially started, using a snapshot of data from the original case management system and Fraud Investigation Reporting System Toolkit (FIRST) used by investigators, with details from Advance Warnings being added gradually over time.
Advance Warnings are produced in respect of forthcoming trials in relation to fraud investigations. The warnings are issued by external Local Counter Fraud Specialists based at NHS organisations or Senior Fraud Investigators from NHSCFA, and circulated where it is anticipated that a fraud case has the possibility of external interest.

NHSCFA Service Desk receive the Advance Warning via a shared HSCA mailbox, and they manually update the HSCA database using details from the Advance Warning. This is the only information used to populate the database. In practice we should be sent details of all Advance Warnings but this is not the case and therefore the database is only as reliable as the information provided to us.

Service Desk receive requests in to the HSCA mailbox to check if a performer has ever been investigated for fraud. They may also receive requests to check if there are any adverse records held on a corporate body; however these are forwarded to be checked in iBase as there is no facility to check corporate bodies in the HSCA database. There are on average approximately 500 HSCA checks requested each month with only 2% having a positive result.

The requests are from NHS England and occasionally from Scotland or Wales where the performer (contractor) was previously registered in England. When there is no fraud matched to the person's name and date of birth, the results of the check are shared by Service Desk with the requester, however where there is found to be a positive match, the information is forwarded to the Information Governance Officer to be investigated further using iBase and for a separate response.

Information in the database could include name, date of birth, registration number and occupation.
The mailbox used in conjunction with the database holds results of checks and details of advance warnings, going back historically in the archive to 2003.

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

    a. Access is restricted to four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist
    b. The HSCA 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

11. Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. However , as the HSCA database was created to record details of individuals who have **EVER** been subject to a fraud investigation, it was not designed to include the date that the record was entered and as such, there is no way of determining how long a record has been there, if it is still relevant or if it is out of date
12. . 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

13. Access is restricted to four members of staff from NHSCFA Service Desk, the Information Governance Officer and the Loss Analysis Specialist

Section 5: External Sharing and Disclosure of Data

14. Results of checks where there is a positive match to an individual having been investigated for fraud are shared with the employing authority who has requested the check.

Section 6: Notice/Signage

15. It would be inappropriate for NHSCFA to advise individuals of their data being processed, as the purpose for processing the data is to record information in relation to individuals who have been subject to an Advance Warning in relation to NHS Fraud Investigations in order to advise NHS employing authorities of any adverse outcomes. Personal data would also be held in the email system as part of the request for a check to be conducted, and would include personal data of individuals who have never been the subject of a fraud investigation. However individuals applying for NHS employment would be aware that pre-employment checks would be conducted.
16. 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.
17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to the HSCA Database and therefore outside the scope of this PIA.

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

18. 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.
19. It is unlikely that many access requests will be received as the personal data recorded is all in relation to fraud investigations that are confidential until such point they are substantiated
20. In the unlikely event that that information in relation to the subject is identified as being incorrect, NHSCFA Service Desk would liaise with the author of the Advance Warning to correct the record.
21. 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

22. The security and technical access architecture of the HSCA 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.

23. Access is restricted to internal staff only.

24. 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

25. The HSCA Database consists of a database holding personal information copied from Advance Warnings and is located in the Counter Fraud Authority data centre.

Conclusion

26. There are no residual privacy risks to the personal data recorded in the HSCA 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 HSCA 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 – HSCA 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	Name, date of birth, professional registration number and occupation	The information is transferred from the Advance Warning to the HSCA Database, and used as a checking mechanism to determine if a health professional applying to be on the contractors list has ever been investigated for fraud. The information would also be held in the email system as part of the request for a check to be conducted, and would include personal data of individuals who have never been the subject of a fraud investigation. The data would not be used for any other purpose.
2	Address, Sensitive Data as listed in Annex A of PIA *Commission or alleged commission of offences for Subjects. *Proceedings relating to an actual or alleged offence for Subjects. *Racial or ethnic origin of Subject	Additional information contained in the Advance Warning itself and retained in the HSCA mailbox.

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	HSCA 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 database was created in 2012 for when the National Health Service (Performers Lists) (England) Regulations 2013 were introduced, and written in to the regulations was the obligation for NHSBSA to check if performers (contractors) i.e Health Professionals, GPs, Dentists Opticians and Pharmacists have ever been investigated for 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 HSCA Database is to have a mechanism of checking if a Health Professional applying for employment within the NHS, has ever been investigated for fraud.

Access is restricted to six members of staff within NHSCFA.

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 HSCA 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: '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. (Data Protection Act, section 1)

NHSCFA offices

Coventry

Cheylesmore House
5 Quinton Road
Coventry
West Midlands
CV1 2WT

02476 245500

London

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

0207 972 2000

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH

0191 204 6303