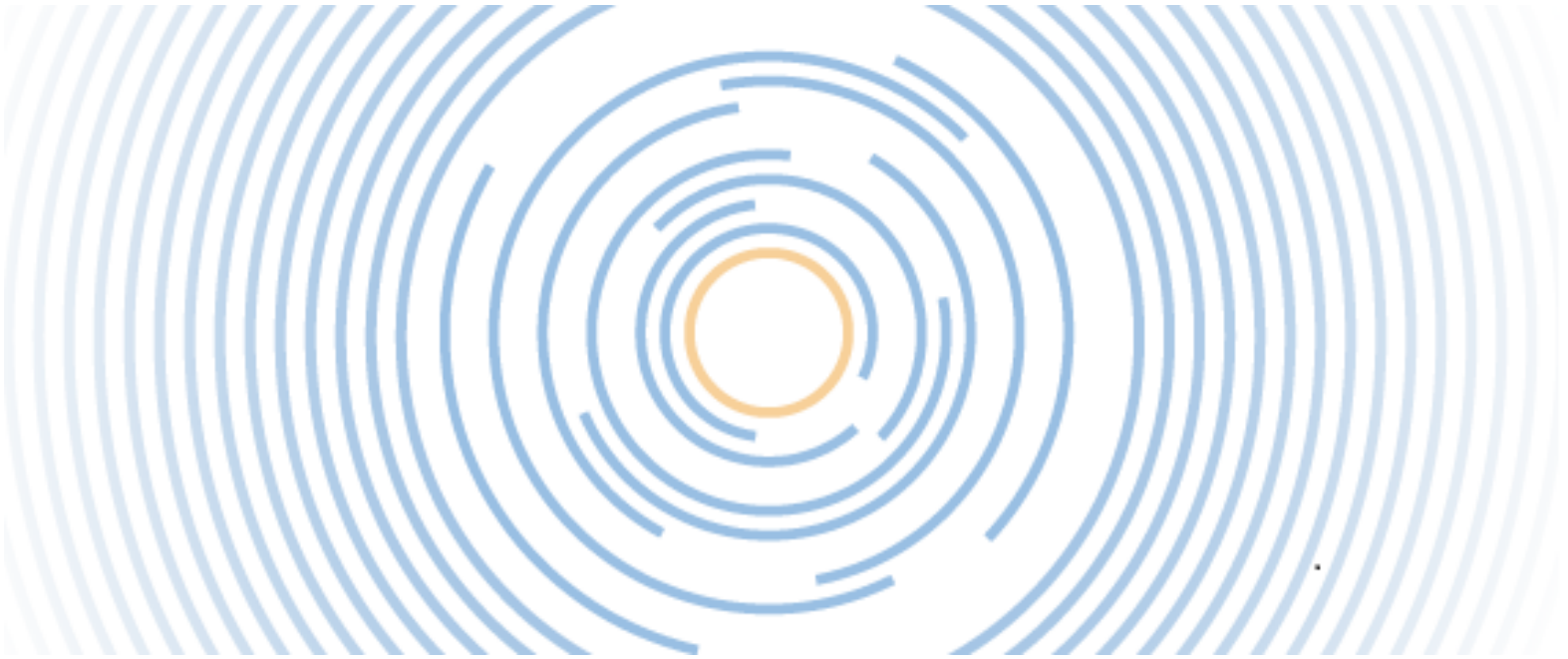
NHS Protect

Information Source Register

Privacy Impact Assessment

V2.0 Published Version

September 2017



Executive summary

This document contains information in relation to a register of persons reporting allegations of fraud, via the Fraud and Corruption Online Reporting Line (FCROL) but who do not wish their personal details to be disclosed. 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'

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

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Information and Records Management Officer	**PIA / Information Source Register**	**DPO**	**V0.1**	**12/09/2017**	**All**
Information and Records Management Officer	**PIA / Information Source Register**	**DPO**	**V0.2**	**27/09/2017**	**Updates from IG Lead**
Information and Records Management Officer	**PIA / Information Source Register**	**DPO**	**V1.0**	**07/03/2019**	**Redacted version prior to publication**
Information and Records Management Officer	**PIA / Information Source Register**	**DPO**	**V2.0**	**13/09/2021**	**Reviewed and anonymised for final publication – no amendments to original version completed in 2017.**

Prefix	
Reference:	**PIA/Information Source Register**
Date:	**September 2017 (original completion date)**
Author:	**Information and Records Management Officer**
Data Owner:	**Strategic Intelligence Lead**
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
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
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
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 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.

Information Source Register General Description

6. The Information Source Register is essentially a spreadsheet that holds the contact details, of persons reporting allegations of fraud, via the Fraud and Corruption Online Reporting Line (FCROL) but who do not wish their personal details to be disclosed. FCROL is managed by Crime stoppers and there are three ways in which a source can make a report. They can do so 'anonymously', 'in confidence' or as a 'named individual'. The choice made by the source will determine the way in which their personal information will be handled. When the source has opted for their information to be held in confidence their personal details are recorded as confidential contacts in a password protected spreadsheet and separated from the allegation itself. Details of the allegation are transferred to the NHS Protect iBase (intelligence) system and linked to the confidential source only via a unique reference number. There is also a password protected mailbox to liaise with the confidential source, together with a second spreadsheet, kept separately to log any communications between the source and the single point of contact in NHS Protect, should it be necessary to obtain permission to pass on their contact details to a Local Counter Fraud Specialist (LCFS) if they wish to initiate an investigation.

7. The Information Source Register was created by NHS Protect in January 2013.

The process involves the management of confidential contact details where the source of information does not want their details to be disclosed, and liaising between the confidential source and the LCFS should an investigation be initiated from the information / allegation of fraud received. On receipt of an allegation of fraud Information is logged to FCROL and then transferred from FCROL to iBase, however where the source requests that their contact details are kept confidential, the contact details aren't transferred, but instead retained separately and emailed securely from crime stoppers to NHS Protect, where they are recorded in the (Information Source Register – confidential contacts) spreadsheet.

8. For security and confidentiality purposes, the register is only accessible by a single point of contact within NHS Protect and one other member of staff.

9. 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.

10. The Information Source Register, 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 NHS Protect adapted Pre Privacy Impact Assessment Questionnaire. 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

11. The following tables describes the Information Source Register roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Strategic Intelligence Lead
Senior Responsible Officer (SRO)	Head of Intelligence and Crime Reduction
Application Owner	Strategic Intelligence 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 NHS Protect 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 NHS Protect 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	Information Source Register
2	What is the main function of the System/Application/Project?	The Information Source Register is essentially a spreadsheet that holds the contact details, of persons reporting allegations of fraud, via the Fraud and Corruption Online Reporting Line (FCROL) but who do not wish their personal details to be disclosed When the source has opted for their information to be held in confidence their personal details are recorded as confidential contacts in a password protected spreadsheet and separated from the allegation itself. Details of the allegation are transferred to the NHS Protect iBase system and linked to the confidential source only via a unique reference number. There is also a password protected mailbox to liaise with the confidential source, together with a second spreadsheet, kept separately to log any communications between the source and the single point of contact in NHS Protect, should it be necessary to obtain permission to pass on their contact details to an LCFS if they wish to initiate an investigation.
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 Information which, if subject to unauthorised release, could cause harm or distress to an individual
4	What [1]personal data is collected? (See Annex A for definitions)	The following personal data is captured by the Information Source Register, please note this is not the full dataset, which is identified fully in Annex B Name Address Email address Contact telephone number Details of employment and occupation.
5	From who is the personal data collected?	The personal data has been collected from the source of the information in respect of an allegation of fraud, and who has requested for their details to be held in confidence .

[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.

6	Why is the personal data being collected?	The data is collected so that the confidential source can be contacted by the NHS Protect single point of contact in the event of an investigation being initiated from the information they have provided.
7	How is the personal data collected?	Data has been provided by the confidential source voluntarily via the Fraud and Corruption Reporting Online (FCROL)
8	Describe all the uses for the personal data (including for test purposes).	The data is used for disclosure to an LCFS or to a regulatory body or law enforcement agency, for assistance in progressing an investigation, but only after permission is obtained from the confidential source. 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 on receipt of an allegation of fraud, the first step would be to establish whether or not the source has previously reported a fraud to NHS Protect.
10	Is the personal data shared within internal organisations?	Access is restricted to a single point of contact and one other person within NHS Protect. In the event that an LCFS wishes to follow up an investigation from the fraud allegation, the single point of contact would obtain the express permission of the confidential source before sharing the personal data. However there may be instances where a regulatory body or LEA has a legal basis on which to request the data, subject to DPA legislation.
11	For each organisation, what personal data is shared and for what purpose?	Personal data would only be shared with the LCFS only after express permission of the confidential source was sought. However, a regulatory body or Law Enforcement Agency (LEA) has a legal basis on which to request data. The data held in the Information Source Register is minimal, and includes name, address, telephone number, email address and employment information. The data would be shared in the event that an LCFS wished to progress an investigation from the fraud allegation received.
12	Is personal data shared with external organisations? (If No go to Q15)	Access is restricted to a single point of contact and one other person within NHS Protect. In the event that an LCFS wishes to follow up an investigation from an allegation, the single point of contact would obtain the express permission of the source before sharing the personal data.

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?	Personal data would only be shared with the LCFS and only after express permission of the confidential source was sought. The data held in the Information Source Register is minimal, and includes name, address, telephone number, email address and employment information. The data would be shared in the event that an LCFS wished to progress an investigation from the fraud allegation received.
15	How is the personal data transmitted or disclosed to internal and external organisations?	The data would be transmitted through a password protected email where access to the mailbox is restricted to two users.
16	How is the shared personal data secured by the recipient?	The Information Source Register is a password protected confidential spreadsheet whereby the data within it can only be accessed by two internal users with the relevant permissions. It is not designed to be accessed externally.
17	Which User group(s) will have access to the system?	Access is restricted to two members of NHS Protect staff only.
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?	Although the register doesn’t use roles to assign privileges, the spreadsheet is password protected and only two staff have access.
20	How are the actual assignments of roles and rules verified according to established security and auditing procedures?	Access is restricted to a single point of contact and one other member of NHS Protect staff.
21	What is the current accreditation of the system?	Official (Sensitive)

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

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)	Approximately 15% of all FCROL records have a confidential source and the spreadsheet currently stores more than 250 personal data records in line with data retention policy.
3	Will [3]sensitive personal data be processed, stored or transmitted by the system/application?	No
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)	Given the nature of the info held I would anticipate that this would be low

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 September 2017, identified the following PIA requirements of using the Information Source Register.

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 NHS Protect 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 Information Source Register, 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 Information Source Register holds personal data for the confidential source, who have reported an allegation of fraud through the Fraud and Corruption Reporting Line (FCROL) and have requested that their personal data is held as confidential.

    a. **The personal data held is:**
        - Name, address, email address and contact details. Also possibly their employment details i.e place of work and job title.

2. The impact level of the Information Source Register was assessed CONFIDENTIAL and access is restricted to a single point of contact and one other person within NHS Protect. In the event that an LCFS wishes to follow up an investigation from the fraud allegation, the single point of contact would obtain the express permission of the confidential source before sharing the personal data.

3. The following measures briefly describe what controls have been implemented to protect the Information Source Register 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 Information Source Register can only be accessed by a single point of contact and one other person within NHS Protect staff and is not accessible externally.

    c. The Information Source Register does not have any direct interconnections with other NHS Protect systems and applications. However a unique reference number is the identifier to link the confidential source to the information held in iBase.

    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 NHS Protect DPO is aware of its existence.

4. It is assessed that there are no residual privacy risks to the personal data used by the Information Source Register. Risks to confidentiality are listed in the Risk table below and documented in the Risk Assessment Report.

5. 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.

6. The privacy risks and associated mitigations are described in Table 4. The IAO is responsible for mitigating the risk as defined in the Information Source Register Assessment Report.

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 collected so that the confidential source can be contacted by NHS Protect single contact in the event of an investigation being initiated from the information provided. It wouldn't 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 Information Source Register is subject to NHS Protect 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.	Relevance of personal data is one of the aspects considered during the PIA review. Personally identifiable personal data recorded in the Register, relates to persons who have reported an allegation of fraud but who wish their personal details to be held in confidence. The data would be covered by the NHS Protect retention period and dependent on whether fraudulent behaviour is detected.
5. There is a risk that the personal data is not accurate or up to date.	Data is limited and has been provided directly by the confidential source. NHS Protect 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 are identified in the Risk Assessment report. 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.	No personally identifiable information will be passed to an external organisation other than to a (Local Counter Fraud Specialist) LCFS to progress an investigation, and only after the express permission of the confidential source has been obtained. See point 11 page 11, - data can be shared with a law enforcement agency or regulatory body but only where they have a lawful basis on which to request it.
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

7. The Information Source Register is essentially a spreadsheet that holds the contact details, of persons reporting allegations of fraud, via the Fraud and Corruption Online Reporting Line (FCROL) but who do not wish their personal details to be disclosed When the source has opted for their information to be held in confidence their personal details are recorded as confidential contacts in a password protected spreadsheet and separated from the allegation itself. Details of the allegation are transferred to the NHS Protect iBase system and linked to the confidential source only via a unique reference number. There is also a password protected mailbox to liaise with the confidential source, together with a second spreadsheet, kept separately to log any communications between the source and the single point of contact in NHS Protect, should it be necessary to obtain permission to pass on their contact details to an LCFS in the event of them initiating an investigation.
8. The data is collated in a spreadsheet.
9. The measures that have been implemented to protect the Personal Data are:
    a. Access is restricted to a single point of contact and one other member of NHS Protect staff.
    b. The Information Source Register does not have a direct interconnection with other NHS Protect systems or applications, however there is a unique reference number to link the confidential source to the information saved in iBase.
    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 retention and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

10. Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. . The retention period for the Information Source Register depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found and no action is taken then its 3 years. The data will be stored in digital format and will be erased, using a CESG approved product (Blanco), from the relevant storage server when no longer required. The IAO is required to review the retention period and any requirement to change must be submitted to the Application Change Board.
11. The current retention schedule as detailed above has been approved by the Data Protection Officer.

Section 4: Internal Sharing and Disclosure of Data

12. Access to the Information Source Register is restricted to a single point of contact and one other person in NHS Protect.

Section 5: External Sharing and Disclosure of Data

13. No personally identifiable information will be passed on to an external organisation other than to a (Local Counter Fraud Specialist) LCFS who needs to progress an investigation, and only after the express permission of the confidential source has been obtained, Or to a law enforcement agency or regulatory body with a lawful basis for disclosure, where disclosure is necessary and proportionate to investigation.

Section 6: Notice/Signage

14. Confidential sources are aware of the data we hold for them as they have provided this information to us themselves, when reporting an allegation of fraud. As such we would not need to advise them of what data we hold. In providing us with their data, they are aware that NHS Protect has a legal obligation and duty of care to protect their identity as a confidential source.

15. NHS Protect hosts a subsection within the NHS Protect website entitled “How we handle data” ,within which this link is a document entitled “Q&A of data management ”. This broadly covers all elements of the NHS Protect usage of data, in a nonspecific manner.
16. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to the Information Source Register and therefore outside the scope of this PIA.

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

17. Individuals have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHS Protect, 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.
18. It is unlikely that many access requests will be received as the personal data in the system is limited and has been provided by the data subject themselves.
19. In the unlikely event that that information in relation to the subject is identified as being incorrect the single point of contact would correct the record.
20. 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

21. The security and technical access architecture of the Information Source Register 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.

22. Access is restricted to a single point of contact and one other NHS Protect staff member.
23. The technical controls to protect the database include:

a. Anti-virus protection;

b. Permission based access controls;

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

24. The Information Source Register consists of a spreadsheet, holding the contact details of individuals who have reported allegations of fraud to NHS Protect, but who wish their data to be held in confidence. The register is located in the NHS Protect/NHS Counter Fraud Authority data centre.

Conclusion

25. There are no residual privacy risks to the personal data recorded in the Information Source Register. 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 Information Source Register, 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 NHSProtect 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 – NHS Protect Information Source Register 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, address, email address and contact telephone number of the confidential source.	The data is collected so that the confidential source can be contacted by the NHS Protect single source of contact in the event of an investigation being initiated from the information they have provided. It would not be used for any other purpose.

Annex C – Data Protection Compliance Check Sheet

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

1. Organisation and project.

Organisation	NHS Protect
Branch / Division	NHS Protect
Project	Information Source Register

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	Business Support, NHS Protect
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhsprotect.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 Information Source Register was introduced in 2013 in order to separate and record in confidence, the contact details of individuals who have reported allegations of fraud. It consists of an electronic log of confidential contacts, linked to the information they have provided only by a unique reference number.

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

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

The purpose of the Information Source Register is to have an electric system designed to record, in confidence, the contact details of individuals who have requested for their details be held confidentially where they have reported an allegation of fraud.

Access is restricted to a single point of contact and one other member of staff within NHS Protect.

The single point of contact would email the source to request permission to share their contact details, should an LCFS wish to follow up an investigation from the information the confidential source had provided.

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 Information Source Register this 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)

NHS Protect 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