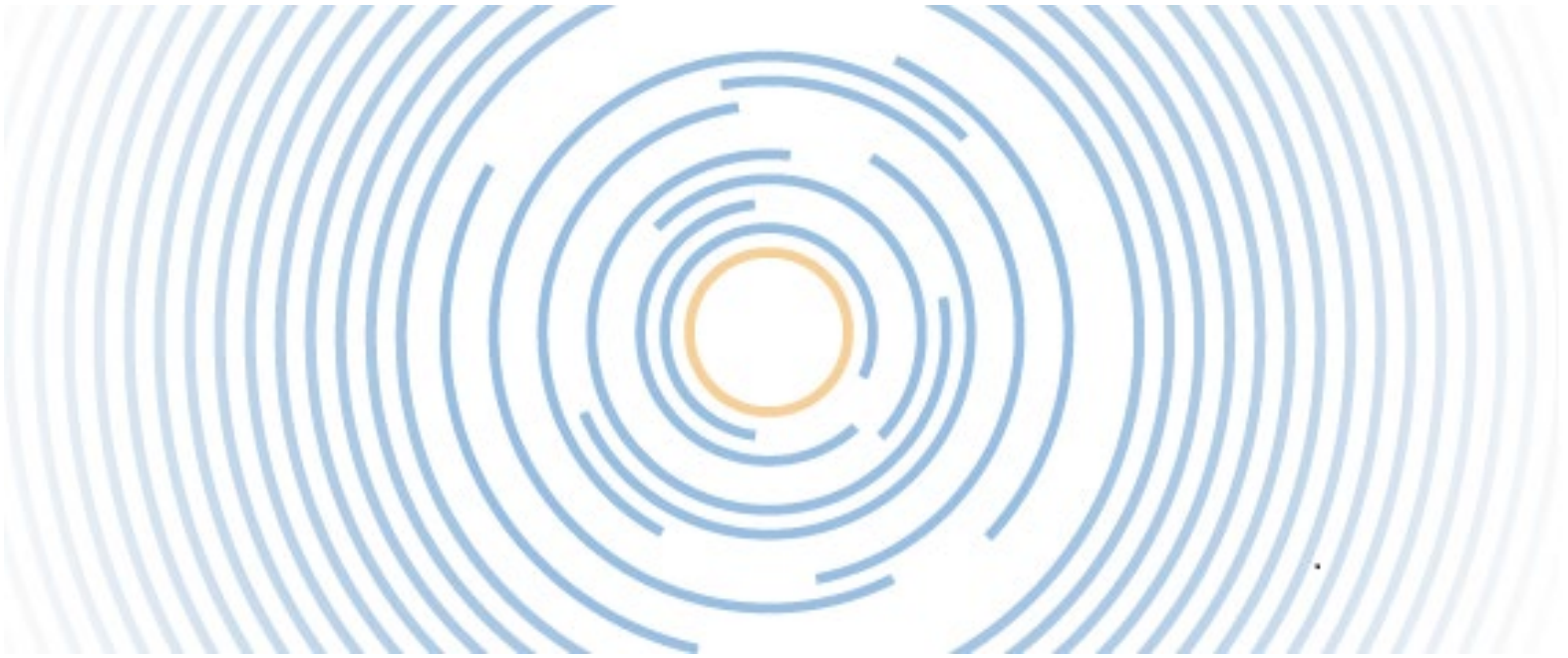
NHS Protect

Press Office Database

Privacy Impact Assessment

V1.0

September 2017



Executive summary

This document contains information in relation to a Press Office Database, comprising of highly sensitive information in relation to notifications of Advance Warnings. The warnings, which are primarily for operational purposes, contain information regarding forthcoming trials and are issued to the Press Office where it is anticipated that an NHS fraud investigation has the possibility of generating external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources. 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 / Press Office Database**	**Trevor Duplessis**	**V0.1**	**28/09/2017**	**All**
Susan Hyde	**PIA/Press Office Database**	**Trevor Duplessis**	**V0.2**	**22/11/2017**	**Amendments from Senior Media Relations Officer**
Susan Hyde	**PIA/Press Office Database**	**Trevor Duplessis**	**V1.0**	**27/03/2019**	**Version amendment prior to publication**

Prefix	
Reference:	**PIA/Press Office Database**
Date:	**September 2017**
Author:	**Susan Hyde**
Data Owner:	**Purdy Sian Davis**
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 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.

Press Office Database General Description

6. The Press Office Database is a database and confidential email system comprising of highly sensitive information in relation to notifications of Advance Warnings. 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 Protect. The warnings are created primarily for operational purposes, circulated to Operational Managers and shared with the Press Office / Media Relations Team where it is anticipated that an NHS fraud investigation has the possibility of generating external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources. The NHS Protect Media Relations Team would be responsible for formulating a press response after successful legal action, normally issued just after sentencing or judgement. The factual content of these press releases are checked and signed-off by the investigators who led the investigation and senior managers. Media Relations staff may provide informal background briefings to the media using information that is already in the public domain, but attributable quotes from NHS Protect are usually from senior NHS Protect officials.

7. The Press Office Database was created by NHS Protect in 2009 to record details of Advance Warnings in respect of Fraud Investigations.

8. The process involves transferring the content of the Advance Warning to a database as a case summary for reference, and would include the subject name and information, summary of the case and any subsequent updates. Contact details of legal and media contacts and also legal and media outcomes. The Media Relations Team can then refer to this information should they need to formulate a press response or locate the information if they receive any queries from the media, or internal, media and stakeholder requests for previous case studies. The confidential mailbox is used for all incoming and outgoing communications in respect of the Advance Warnings and subsequent press releases.

9. For security and confidentiality purposes, the database is normally only accessed by two members of staff from NHS Protect Media Relations Team.

10. 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.

11. The Press Office 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 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

12. The following tables describes the Press Office Database roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Purdy Sian Davis
Senior Responsible Officer (SRO) Information Risk Owner (IRO)	Purdy Sian Davis
Application Owner	Gary Blackhurst
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 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	Press Office Database
2	What is the main function of the System/Application/Project?	The Press Office Database is a database and confidential email system comprising of highly sensitive information in relation to notifications of Advance Warnings. The warnings which are primarily for operational purposes 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 Protect. The warnings are circulated to Operational Managers and shared with the Media Relations Team / Press Office where it is anticipated that an NHS fraud investigation has the possibility of generating external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources. The NHS Protect Media Relations Team would be responsible for formulating a press response after successful legal action, normally issued just after sentencing or judgement. The factual content of these press releases are checked and signed-off by the investigators who led the investigation and senior managers. Media Relations staff may provide informal background briefings to the media using information that is already in the public domain, but attributable quotes from NHS Protect are usually from senior NHS Protect officials. The data in the Press Office Database is also used for proactive media relations, for example where case studies may be requested for use in a TV documentary.
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 could be potentially included in the Advance Warning and subsequently transferred to the Press Office Database, please note this is not the full dataset, which is identified fully in Annex B **For subject of AW:** Name, Address & Contact details of Subject Date of birth of Subject Nationality and NI number of Subject. Passport Number of Subject. NHS Number of Subject Driving Licence Number of Subject. Payroll Number of Subject. Professional Body Subject registered to. Professional Registration Number of Subject. NHS Employment / links to NHS for subject Details of NHS Department to where subject may be attending for treatment. Detailed description of Subject. Bank details of Subject. Details of credit history and personal checks Vehicle details of Subject. Outcome relating to an offence for Subject Company Name (Non-NHS Subject only) SIC Code (Non-NHS Subject only) Registration Number (Non-NHS Subject only) Incorporation Date (Non-NHS Subject only) VAT Number (Non-NHS Subject only) Trading Address and Registered Address (Non-NHS Subject only ***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 the above, business card information is also collected from the author of the Advance Warning and from external media relations personnel who have an interest in the case.
5	From who is the personal data collected?	The personal data 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 NHS Protect.

[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 as a reference database for the Media Relations Team, who can then refer to the information should they need to formulate a press response or locate the information if they receive any queries from the media, or internal, media and stakeholder requests for previous case studies.
7	How is the personal data collected?	Information is transferred to the database from the Advance Warnings.
8	Describe all the uses for the personal data (including for test purposes).	The data is used to formulate a press release However although personal and sensitive personal data is processed, information not cleared as suitable for public disclosure would not be included in the press release. 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 used to search for specific information and reports can be generated from the results.
10	Is the personal data shared within internal organisations?	Access is normally restricted to two members of staff from the NHS Protect Media Relations team only. Copies of the Advance Warning might occasionally be requested by and shared with Senior colleagues from NHS Protect even though they are already on the circulation list to receive them.
11	For each organisation, what personal data is shared and for what purpose?	Access is normally restricted to two members of staff from the NHS Protect Media Relations team only.
12	Is personal data shared with external organisations? (If No go to Q15)	Access is normally restricted to two members of staff from the NHS Protect Media Relations team only.
13	Is personal data shared with external organisations that are not within the [2]European Economic Area?	No

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

14	For each external organisation, what personal data is shared and for what purpose?	The data is used to formulate a press release However although personal and sensitive personal data is processed, information not cleared as suitable for public disclosure would not be included in the press release. Senior colleagues might occasionally ask the Media Relations Team / Press Office for a copy of an Advance Warning, even though they are on the circulation list to receive that particular AW. We don't ever send an Advance Warning verbatim to the media, even after a successful prosecution.
15	How is the personal data transmitted or disclosed to internal and external organisations?	The data would be transmitted by way of a press release, through a confidential email account where access to the mailbox is restricted to two users.
16	How is the shared personal data secured by the recipient?	The Press Office Database is a bespoke application whereby the data within it can only be accessed by users with the relevant permissions, and although it can be accessed by all members of the Organisational Development team, there is an understanding that only two members of staff should access it. It is not designed to be accessed externally.
17	Which User group(s) will have access to the system?	Although it can be accessed by all members of the Organisational Development team, there is an understanding that only two members of staff should normally access it. 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?	Although the database doesn't use roles to assign privileges, there is an understanding that only two members of staff from the Media Relations team should access the database.
20	How are the actual assignments of roles and rules verified according to established security and auditing procedures?	Access is restricted to staff from the Media Relations team and line management only. 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 September 2017, identified the following PIA requirements of using the Press Office 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 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 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:

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 Press Office 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 Press Office Database holds highly sensitive personal data and information transferred directly from Advance Warnings. Advance Warnings are produced primarily for operational purposes and are shared with the Press Office where it is anticipated that a fraud case has the possibility of external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources.

    a. **The following personal data could potentially all be included in the Advance Warning and subsequently transferred to the database:**
    For the subject of the Advance Warning:
    Name, address, date of birth, contact details, nationality, NI number, passport number, racial or ethnic origin, NHS number, driving licence number, payroll number, details of professional body including registration number, NHS employment details or any links to NHS including department where treatment is being received, details of any other occupation/employment, detailed description of subject, Bank Details including name, address and phone number, sort code and account number, Vehicle Details including make, model, colour, age and licence registration plate. Racial or ethnic origin, Details of any commission or alleged commission of offences, Proceedings and outcomes relating to an actual or alleged offence, Details of credit history and other personal checks

    b. In addition to the above, business card information is also collected from the author of the Advance Warning and from external media relations personnel who have an interest in the case.

2. The impact level of the Press Office Database was assessed as CONFIDENTIAL and although it can be accessed by all members of the Organisational Development team, there is an understanding that only two members of staff should normally access it.

3. The following measures briefly describe what controls have been implemented to protect the Press Office 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 Press Office Database will only be accessed by two members of staff within the Media Relations Team.

    c. The Press Office Database does not have any direct interconnections with other NHS Protect 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 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 Press Office Database. Risks to confidentiality are listed in the Risk table below.

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.

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 recorded as a reference in the event that a press release has to be formulated. It may also be used for other publicity products for example if a case study was requested for a TV documentary.
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 Press Office Database is subject to NHS Protect Data Handling and Storage Policy and will be audited annually to ensure 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 Press Office Database, relates to persons who are subject to an Advance Warning and where a press release may be published. The data would be covered by the NHS Protect retention period which for the Press Office Database is 7 years
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 NHS Protect. 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. The information from the Advance Warning is transferred exactly in its entirety to the Press Office Database. 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 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.	No personally identifiable information will be passed on to an external organisation, unless it is already in the public domaim.
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 Press Office Database is a database and confidential email system comprising of highly sensitive information in relation to notifications of Advance Warnings. The warnings are produced primarily for operational purposes and contain information regarding forthcoming fraud trials. They are issued by external Local Counter Fraud Specialists based at NHS organisations or Senior Fraud Investigators from NHS Protect. The warnings are circulated to Operational Managers and shared with the Media Office / Press Office where it is anticipated that an NHS fraud investigation has the possibility of generating external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources. The NHS Protect Media Relations Team would be responsible for formulating a press response.

8. The data is collated in a database.

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

   a. Access is restricted to staff in the NHS Protect Media Relations team only.

   b. The Press Office database does not have a direct interconnection with other NHS Protect 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

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 Press Office Database is 7 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. Although the Press Office Database can be accessed by all members of the Organisational Development team, there is an understanding that only two members of staff should access it.

Section 5: External Sharing and Disclosure of Data

13. No personally identifiable information will be passed on to an external organisation unless it is already in the public domain or it is considered appropriate to share with wider the NHS, for example Trust Communications Departments.

Section 6: Notice/Signage

14. It would be inappropriate for NHS Protect to advise individuals of their data being processed, as the purpose for processing the data is to record fraudulent behaviour that is subject to an Advance Warning containing information regarding forthcoming trials, where it is known that a fraud case has the possibility of external interest, the potential for press coverage, or that the press may become aware of a particular investigation through other sources.

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 Press Office Database 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 recorded is all in relation to fraud investigations that are confidential until such point they are substantiated
19. In the unlikely event that that information in relation to the subject is identified as being incorrect the author of the Advance Warning would correct the information, which would subsequently be updated in the database. The Press Office would correct any records they have generated themselves.
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 Press Office 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.

22. Access is restricted to staff from the Organisational Development team only.
23. 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

24. The Press Office Database consists of an a database holding information transferred verbatim from Advance Warnings and also holds some additional notes. It 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 Press Office 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 Press Office 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 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 Press Office 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, Address & Contact details Date of birth Nationality and NI number. Passport Number. NHS Number Driving Licence Number Payroll Number. Professional Body Subject registered to Professional Registration Number NHS Employment / links to NHS Details of NHS Department to where subject may be attending for treatment. Detailed description. Bank details. Details of credit history and personal checks Vehicle details. Outcome relating to an offence. Company Name (Non-NHS Subject) SIC Code (Non-NHS Subject only) Registration Number (Non-NHS Subject only) Incorporation Date (Non-NHS Subject only) VAT Number (Non-NHS Subject only) Trading Address and Registered Address (Non-NHS Subject only ***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*	The information is transferred from the Advance Warning in its entirety to the Press Office Database. The data is required in the event that a press response is required. However, caution would be applied in formulating the press response to ensure that limited personal data is included. The data is also used for proactive media relations, for example as case studies in a TV documentary.
2	In addition to the above, business card information is also collected from the author of the Advance Warning and from external media relations personnel who have an interest in the case.	In order to make contact with the author of the AW or with the media.

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	Press Office 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	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 NHS Protect Press Office Database was created in 2009 to record details of Advance Warnings in respect of fraud investigations. Advance Warnings are issued primarily for operational purposes in relation to forthcoming trials, and are shared with the press office and with other senior colleagues in NHS Protect where it is anticipated that a fraud case has the possibility of external interest and a press release needs to be formulated.

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 Press Office Database is to have a reference to information from the Advance Warnings should it be necessary to formulate a press response.

Access is restricted to staff within the Organisational Development Team but it there is an understanding that only two people should normally access it.

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 Press Office 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)

NHS Protect 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