

OFFICIAL

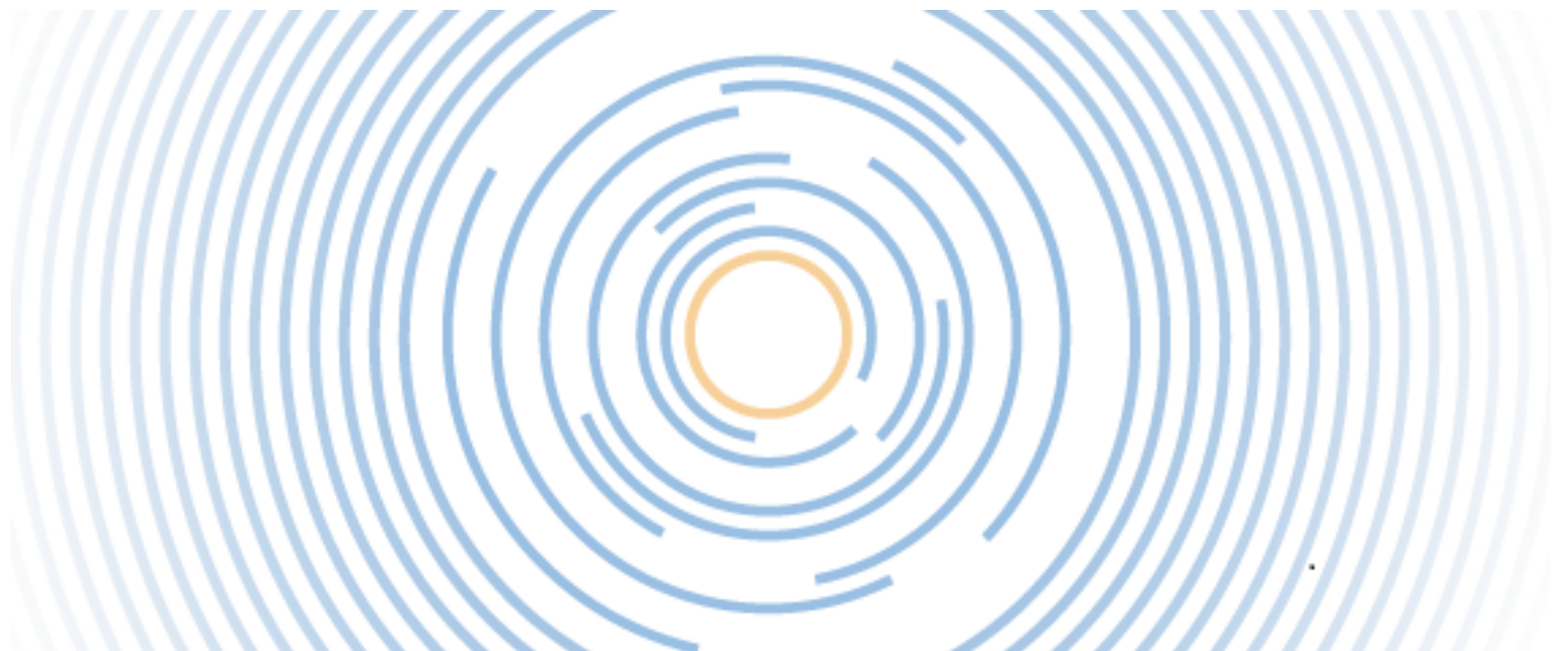


# **NHS Protect Complaints Process**

## **Privacy Impact Assessment**

**V1.0 Published Version**

**September 2017**



**Leading the NHS fight against crime**

# Executive summary

**This document contains information in relation to the managing of informal and formal complaints to NHS Protect in relation to its staff, or its services or processes and as such it is deemed OFFICIAL.**

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](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'

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

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

## Table of contents

<b>Table of contents .....</b>	<b>3</b>
<b>Links &amp; Dependencies .....</b>	<b>5</b>
<b>Table 1 – Links and Dependencies .....</b>	<b>5</b>
<b>Section 1: .....</b>	<b>6</b>
<b>Privacy Impact Assessment Requirement &amp; Process.....</b>	<b>6</b>
<b>Introduction.....</b>	<b>6</b>
<b>PIA Phases .....</b>	<b>6</b>
<b>NHS Protect Complaints Process General Description .....</b>	<b>7</b>
<b>Ownership .....</b>	<b>7</b>
<b>Section 2: PIA Screening .....</b>	<b>8</b>
<b>The PIA Screening Process .....</b>	<b>8</b>
<b>Screening Process Conclusions .....</b>	<b>10</b>
<b>Section 3: PIA Report .....</b>	<b>13</b>
<b>Section 4: Compliance Checks.....</b>	<b>17</b>
<b>DPA 98 Compliance Check .....</b>	<b>17</b>
<b>The Privacy and Electronic Communications Regulations .....</b>	<b>17</b>
<b>The Human Rights Act 1998 .....</b>	<b>17</b>
<b>The Freedom of Information Act .....</b>	<b>17</b>
<b>Annex A - Definition of Protected Personal Data.....</b>	<b>18</b>
<b>Annex B – NHS Protect Complaints Process Personal Data .....</b>	<b>19</b>
<b>Annex C – Data Protection Compliance Check Sheet.....</b>	<b>20</b>

OFFICIAL

Document Control					
PM	Ref	Document owner	Version No	Issue Date	Amendments
Information and Records Management Officer	PIA NHS Protect Complaints Process	DPO	V0.1	04/09/2017	All
Information and Records Management Officer	PIA NHS Protect Complaints Process	DPO	V0.2	20/09/2017	Amendments following review by DPO
Information and Records Management Officer	PIA NHS Protect Complaints Process	DPO	V1.0	19/10/2021	Reviewed and anonymised for final publication – slight amendments to original version completed in 2017 <b>see addendum</b>

Addendum – addition/deletion of words	
<b>Page 7</b> point 6	<b>(additions)</b> may also be shared with Intelligence/Operations and Quality & Compliance staff where the provision of a corporate response to a particular issue requires specialist knowledge and where we need to confirm if the complaint is in relation to a live investigation, or if an internal review is to be conducted.
<b>Page 9 &amp; 10</b> Points 10 &11	<b>(addition)</b> and Quality & Compliance staff
<b>Page 10</b> Point 17	<b>(deletion)</b> Organisational Development Team and Intelligence / Operations Team/.
<b>Page 11</b> Point 20	<b>(deletion)</b> and Intelligence / Operations Team. <b>(addition)</b> The Chief Executive <b>(deletion)</b> Managing Director

Prefix	
Reference:	PIA/NHS Protect Complaints Process
Date:	September 2017 (original completion date)
Author:	Information and Records Management Officer
Data Owner:	Organisation Development Officer
Version:	1.0
Supersedes	0.2

## Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	1998	HMG
EU GDPR	EU General Data Protection Regulation	All	May 2018	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	April 2014	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

**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.

## NHS Protect Complaints Process General Description

6. The NHS Protect Complaints Process is an electronic log of informal and formal complaints consisting of a spreadsheet and a folder of corresponding communications. The NHS Protect definition of a complaint is: **“An expression of dissatisfaction that requires a response”**. This includes dissatisfaction about the service provided, including the conduct of staff, or the process involved in deciding what action to take (or not to take). Complaints can include claims of unfair treatment by NHS Protect, dissatisfaction about how NHS Protect has dealt with a situation, claims that a poor standard of service has been provided and claims that NHS Protect staff have been unhelpful or rude. Access to the Complaints Process is restricted to a small number of staff and line management within the Organisational Development Team. However information may also be shared with Intelligence/Operations and Quality & Compliance staff where the provision of a corporate response to a particular issue requires specialist knowledge and where we need to confirm if the complaint is in relation to a live investigation, or if an internal review is to be conducted.
7. The NHS Protect Complaints Process was created by NHS Protect in 2006 in support of the BSA complaints policy
8. The process involves the central management of complaints against NHS Protect staff, or its services and processes, and collating files of corresponding information relating to each complaint.
9. The system is only accessible by a limited number of NHS Protect staff.
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 NHS Protect Complaints Process, 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 NHS Complaints Process roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Organisation Development Manager
Senior Responsible Officer (SRO) Information Risk Owner (IRO)	Head of Intelligence and Crime Reduction
Application Owner	Senior Compliance and Complaints Officer
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	NHS Protect Complaints Process
2	What is the main function of the System/Application/Project?	The NHS Protect Complaints Process is an electronic log of informal and formal complaints consisting of a spreadsheet and a folder of corresponding communications. Complaints can include claims of unfair treatment by NHS Protect, dissatisfaction about how NHS Protect has dealt with a situation, claims that a poor standard of service has been provided and claims that NHS Protect staff have been unhelpful or rude.
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



## OFFICIAL

<b>4</b>	What <sup>1</sup> personal data is collected? (See Annex A for definitions)	The following personal data is captured by NHS Protect Complaints Process, please note this is not the full dataset, which is identified fully in Annex B Name Address Email Address Contact Details Details of NHS Employment and Occupation.
<b>5</b>	From who is the personal data collected?	The personal data has been collected from the complainant or their representative.
<b>6</b>	Why is the personal data being collected?	The data has been collected to allow for complaints to be recorded and is necessary as a reference to support the formal response process.
<b>7</b>	How is the personal data collected?	Data has been provided by the claimant or their representative voluntarily by way of a telephone call, email or letter.
<b>8</b>	Describe all the uses for the personal data (including for test purposes).	The data is used for the purpose of resolving complaints by responding with either an explanation, an apology or advise of any conclusions and action.  Data is not used for test purposes.
<b>9</b>	Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern?	Having electronic data allows the Organisational Development Team to identify emerging themes, learn from the complaints reporting mechanism and have an awareness of escalated complaints.
<b>10</b>	Is the personal data shared within internal organisations?	Access is restricted to a small number of staff and line management within the Organisational Development Team. However, information may also be shared with Intelligence / Operations and Quality & Compliance staff where the provision of a corporate response to a particular issue requires specialist knowledge and where we need to confirm if the complaint is in relation to a live investigation.

---

<sup>1</sup> 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.

OFFICIAL

11	For each organisation, what personal data is shared and for what purpose?	Information may be shared with Intelligence/Operations/Quality & Compliance staff where the provision of a corporate response to a particular issue requires specialist knowledge and where we need to confirm if the complaint is in relation to a live investigation.
12	Is personal data shared with external organisations? (If No go to Q15)	Where complaints are received that are not within our remit, we may have to forward the information to the appropriate NHS trust/ organisation. Where a complaint is escalated to stage 2 of the complaints process, previous correspondence / information is often shared with the DH Sponsor to assist in answering the complaint.
13	Is personal data shared with external organisations that are not within the <sup>2</sup> European Economic Area?	No
14	For each external organisation, what personal data is shared and for what purpose?	Where complaints are received that are not within our remit, we may have to forward the information to the appropriate NHS trust/ organisation. Where a complaint is escalated to stage 2 of the complaints process, previous correspondence / information is often shared with the DH Sponsor to assist in answering the complaint.
15	How is the personal data transmitted or disclosed to internal and external organisations?	Access to the data is restricted to a limited number of internal staff and line management only. The data would be accessed via permissions to a folder, or emailed via secure mail.
16	How is the shared personal data secured by the recipient?	NHS Protect Complaints Process is a bespoke application whereby the data within it can only be accessed by 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?	Organisational Development Team Systems Administrators

<sup>2</sup> Norway, Iceland and Lichtenstein together with other European Union Nations and Switzerland make up the European Economic Area.

## OFFICIAL

<b>18</b>	Will contractors/service providers to NHS Protect have access to the system?	No
<b>19</b>	Does the system use “roles” to assign privileges to users of the system?	Although the system doesn’t use roles to assign privileges, there is only a limited number of staff who access the data.
<b>20</b>	How are the actual assignments of roles and rules verified according to established security and auditing procedures?	Access is restricted to staff and line management from the Organisational Development Team  The Chief Executive will have access and review draft responses to all complaints.  System administrators also have full access to all data.
<b>21</b>	What is the current accreditation of the system?	OFFICIAL

**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)	There are approximately only 200 records held, however this will increase in time as more complaints are received.
3	Will <sup>3</sup> 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 that no sensitive personal data is processed, this will be of a lower scale.

<sup>3</sup> 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.

Table 3 – PIA Decision Criteria

## Screening Process Conclusions

5. The screening process, completed in September 2017, identified the following PIA requirements of using the NHS Protect Complaints Process.
  - 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](http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/26-report.html)
  - 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 NHS Protect Complaints Process, including the purposes for which it is gathered and outputs it produces. Documenting evidence of the considerations surrounding potentially contentious elements (i.e. personal data in relation to subjects) can provide further assurance.

## Section 3: PIA Report

### Data Collection and Maintenance

1. The NHS Protect Complaints Process holds personal data on the complainant or their representatives, for complaints made against NHS Protect staff, the services they provide or the processes they have followed.
  - a. **For the complainant.**
    - Name, address, email address and contact details. Also possibly their employment details i.e place of work and job title.
  - b. **For the representative including MP.**
    - Name, address, email address and contact details.
  - c. **For subject of a complaint that may be out of our remit.**
    - Name, details of NHS employment and occupation.
2. The impact level of the NHS Protect Complaints Process was assessed CONFIDENTIAL and the information is only accessed internally, unless the complaint is escalated to stage 2 of the complaints process whereby it would be shared with DH Anti Fraud Unit.
3. The following measures briefly describe what controls have been implemented to protect the NHS Protect Complaints Process and the personal data recorded:
  - a. All off site back-ups are secure as they can only be opened via the encryption key.
  - b. NHS Protect Complaints Process is only available to a limited number of internal NHS Protect staff and is not accessible externally.
  - c. NHS Protect Complaints Process does not have any direct interconnections with other NHS Protect systems and applications.
  - d. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the 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 NHS Protect Complaints Process. 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 Risk 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 has been collected to allow for complaints to be recorded and is necessary as a reference to support the formal response process. 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 NHS Protect Complaints Process 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 Complaints Process relates to individuals or their representatives who have made a complaint against NHS Protect staff, including its services and processes. As such the data will be relevant whilst the complaint is live. Once the complaint is closed, the data would be covered by the NHS Protect retention period. The organisation's current retention schedule states letters from complainants should be kept for 8 years.
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 complainant or their representative via telephone call, email or letter. 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 external organisation other than for the administration of justice.
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 NHS Protect Complaints Process relates to individuals or their representatives who have made a complaint against NHS Protect staff, including its services and processes. The system holds information on complainants and any individuals who are representing them, details of the complaint itself and the persons of whom the complaint is against.
8. The data is collated in a spreadsheet and an electronic filing system. Any hard copies of correspondence are locked away in filing cabinets.
9. The measures that have been implemented to protect the Personal Data are:
  - a. Access is restricted to a limited number of NHS Protect staff and management only.
  - b. The NHS Protect Complaints Process 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 organisation's current retention schedule states letters from complainants should be kept for 8 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 NHS Protect Complaints Process is restricted to a limited number of internal staff and line management.

## Section 5: External Sharing and Disclosure of Data

13. No personally identifiable information will be passed on to external organisation other than for the administration of justice

## Section 6: Notice/Signage

14. Complainants and representatives are aware of the data we hold for them as they have provided it by way of an email, letter or telephone call. However, It would not be reasonable to notify other individuals of whom there has been a complaint made, as this may include an allegation of fraud which is handled as a referral and be subject to an investigation. Therefore notification may result in behaviours changing/ becoming more complex and as a result be harder to detect.
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 this 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 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 administrators 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 NHS Protect Complaints Process is as explained in this PIA:  

The application and the hosting infrastructure was assessed at Official and the hosting infrastructure is subject to CESG approved IT Security Health Check.
22. Access is restricted to a limited number of NHS Protect staff and line management are responsible for authorising access.
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 NHS Protect Complaints Process is an electronic log of informal and formal complaints against NHS Protect staff, its services and its processes, and 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 NHS Protect Complaints Process. 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 NHS Protect Complaints Process, 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 NHS Protect 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 Complaints Process 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 complainant	The data has been collected to allow for complaints to be recorded and is necessary as a reference to support the formal response process. .
2	Name, address, email address and contact telephone number of representative.	The data has been collected to allow for complaints to be recorded and is necessary as a reference to support the formal response process. .
3	Name and details of NHS employment for subject of complaint that is out of our remit.	The data has been collected to allow for complaints to be recorded and referred to the correct department/NHS Trust for the administration of justice.

## Annex C – Data Protection Compliance Check Sheet

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

#### 1. Organisation and project.

Organisation	NHS Protect
Branch / Division	NHS Protect
Project	NHS Protect Complaints Process.

#### 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.

<p>The NHS Protect Complaints Process was introduced in 2006 to support the Business Service Authorities formal complaints policy. It consists of an electronic log of informal and formal complaints against NHS Protect or its employees, together with a separate folder of complaints that are out of our remit.</p>
--

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

<p>NHS Protect leads on a wide range of work to protect NHS staff and resources from crime.</p> <p>The purpose of the NHS Protect Complaints Process is to have an electric system designed to record, document and manage any complaints made to NHS Protect about the organisation or its employees.</p> <p>Access is restricted to a limited number of staff and management within NHS Protect only, but may be shared with DH if the complaint is not resolved in the first stage of the process and has to be escalated to second stage.</p> <p>Additionally any complaints received that are not within our remit, may be shared with the relevant NHS organisation for the administration of justice.</p>
--

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

Privacy impact assessments have been considered in the light of personal data gathered particularly in relation to alleged offenders. However 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 process.

**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

4<sup>th</sup> Floor  
Skipton House  
80 London Road  
London  
SE1 6LH

### Newcastle

1<sup>st</sup> Floor  
Citygate  
Gallowgate  
Newcastle upon Tyne  
NE1 4WH