Protect

Central Person and Organisation Database (CPOD)

Privacy Impact Assessment

Version 2.0 Published

This document contains mainly 'Business Card' Information in relation to individuals employed to investigate fraud within the NHS. As such, because there is no sensitive data included within the information, this PIA is marked as OFFICAL.

Any information viewed/obtained within this document should therefore 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'

Document Information	
Document Title	CPOD Privacy Impact Assessment
Author	Information and Records Management Officer
Date	May 2017

Document Control					
PM	**Ref**	**Owner**	**Version No**	**Issue Date**	**Amendments**
Information and Records management Officer	PIA/CPOD/ 2017	Head of Business Support	V0.1	03/05/17	All
Information and Records management Officer	PIA/CPOD/ 2017	Head of Business Support	V0.2	08/06/17	Review for typos and amendments
Information and Records management Officer	PIA/CPOD/ 2017	Head of Business Support	V0.3	08/08/2017	Further amendments following review by DPO
Information and Records management Officer	PIA/CPOD/ 2017	Head of Business Support	V1.0	07/03/2019	Minor amendments prior to publication
Information and Records management Officer	PIA/CPOD/ 2017	Organisational Development Manager	V2.0	05/11/2021	Reviewed and anonymised for final publication - no amendments to original version completed in 2017

Preface

Central Person and Organisation Database (CPOD)

Reference:	PIA/CPOD/2017
Date:	May 2017
Author:	Information and Records Management Officer
Owner:	Head of Business Support
Version:	2.0
Supersedes:	1.0

Contents List

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

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 holding data on more than 250 people will require a PIA.

2. The PIA is a process that enables organisations to anticipate, identify 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. Within NHS Protect all systems that process or store personal data on more than 250 people require a PIA to be conducted and documented as part of the accreditation evidence. This PIA is related to, and makes reference to, the NHS Protect RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS also contains the initial PIA completed on creation of this system, which this document supersedes. The RMADS was developed in accordance with the requirements of NHS Protect and CESG HMG Infosec Standards 1 and 2.

CPOD General Description

4. The Central Person and Organisation Database was developed to centralise the person and organisation data held by NHS Protect in one single source and to which other NHSProtect applications could refer. The system was created as a solution to the previous manual process which involved maintaining the contact information in a number of different systems.

CPOD holds details of internal staff and is also predominant to the nomination process for external Local Counter Fraud Specialists and Directors of Finance, and also Audit Committee Chair's in line with the NHS Protect SRT process (Self Reporting Tool) The system also holds records of NHS organisations which are imported on a monthly basis as part of an automatic process.

Accredited Local Counter Fraud Specialists and Directors of Finance must be nominated by the organisation for which they have responsibility before they are granted access to NHS Protect systems and applications, and the first step in the nomination process is to add their details to CPOD.

CPOD is owned and operated by NHS Protect. It is updated and maintained by staff for use as an internal and external contact directory as well as facilitating a process in which to verify and approve access to other NHS Protect systems, by way of verifying security questions and providing individual passwords that stored within the application

5. CPOD 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 CPOD 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

6. The following tables describes CPOD roles and responsibilities:

Role	Responsibility
Information Asset Owner (IAO)	Organisational Development Officer
Senior Responsible Officer (SRO)	Head of Intelligence and Crime Reduction
Application Owner	Head of Business Support
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	Central Person and Organisation Database (CPOD)
2	What is the main function of the System/Application/Project?	The purpose of CPOD (Central Person Organisation Database) is to centralise the person and organisation data held by NHSP in a single database that allows easier maintenance and access to consistent data for all NHSP IT applications. Updated and managed by internal staff, it is used as verification for access to be granted to other NHSProtect systems. The following systems currently utilise CPOD for data: SRT (Self Review Tool) FIRST (Fraud Information and Reporting System Toolkit.
3	Briefly, what are the personal data elements used by the System/Application/Project? See Annex A for guidance,	Information that can be used to identify a living person

4	What [1]personal data is collected? (See Annex A for definitions)	**The following personal data is captured by CPOD** Name Date of birth Contact telephone number Email address Employment Details Propriety dates Training dates Responses to security questions Individual user ID and passwords
5	From who is the personal data collected?	The personal data is collected by NHS Protect either by the individual themselves, from an external nomination form or from internal staff records.
6	Why is the personal data being collected?	The data is collected to ensure consistent contact information is held across NHSProtect systems and also to facilitate a process whereby access to those systems can be granted based on the permissions recorded for individuals.
7	How is the personal data collected?	Data is input manually via the internal CPOD application.
8	Describe all the uses for the personal data (including for test purposes).	Section 6 summarises for what purpose the data is collected. This is explained again below: To maintain a central source of consistent contact information, for access by NHS Protect staff. To be referred to by other NHSProtect systems Used as verification (based on permissions) to allow access to NHSProtect applications. There is no use of personal data for testing
9	Does the system analyse the personal data to assist Users in identifying previously unknown areas of note, concern or pattern?	No
10	Is the personal data shared within internal organisations?	All internal staff can access the data.

[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.

11	For each organisation, what personal data is shared and for what purpose?	All of the personal data identified in section 4 is accessible internally with NHS Protect staff. The purpose as described in section 8 is to ensure that there is a consistent database of contacts. As such, staff can access the data for their own use as well as specific staff using the information to grant external users access to other systems.
12	Is personal data shared with external organisations? (If No go to Q15)	Potentially, however the only information that would be shared would be the names of any nominated /accredited persons within their own organisation.
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?	The only information that might be shared would be the names of any nominated /accredited persons within the same organisation.
15	How is the personal data transmitted or disclosed to internal and external organisations?	Access to the data in CPOD is only accessible internally to NHS Protect staff via the application.
16	How is the shared personal data secured by the recipient?	CPOD is an application whereby the data within it can only be accessed by internal users with the relevant permissions. It is not designed to be accessed eternally.
17	Which User group(s) will have access to the system?	CPOD is an application whereby the data within it can only be accessed by internal users with the relevant permissions. All NHS Protect staff will have different permissions of access.
18	Will contractors/service providers to NHS Protect have access to the system?	No
19	Does the system use “roles” to assign privileges to users of the system?	Yes

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

20	How are the actual assignments of roles and rules verified according to established security and auditing procedures?	NHS Protect Staff Access to the data in CPOD is only accessible internally to NHS Protect staff. Permissions are assigned to staff dependant on their role and whether they require read only access for information or full access to input information and grant access to other systems. System administrators have full access to all data.
21	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)	Yes
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)	Full

[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 May 2017, identified the following PIA requirements of using the CPOD application.

a. 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. A number of legal requirements apply to CPOD and are referenced and included in the Risk Assessment Report and all operating procedures and therefore must be included within this PIA in a manner that is consistently applied. The relevant applicable legislation is:

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 CPOD system, 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: Privacy Impact Assessment & Process

Introduction

1. 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. 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.

2. The PIA screening process concluded in 2017 that although not undertaken at the beginning of the project, a requirement for a Full PIA was required based on the type and quantity of personal data involved.

PIA Phases

3. 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.

Approach

4. CPOD was designed and built by NHS Protect as a solution to hold consistent personal information and organisation data in one central database. It became partially operational amongst NHS Protect staff in December 2012 with full delivery following by 2014. This is the first Privacy Impact Assessment on the system and as such, all content, considerations and assessments are based on existing arrangements in place within NHS Protect for similar datasets.

5. CPOD is a system used by internally by NHSProtect staff and is in continuous development since its introduction. This PIA is developed by the Information Analytics Lead, in consultation with NHSProtect staff from a number or teams.

Section 4: PIA Report

Executive Summary

1. The CPOD System records personal data on internal staff and external Local Counter Fraud Specialists and Directors of Finance. This information includes the following:

    - Name
    - Date of birth,
    - Employment details
    - Contact telephone number
    - Email address
    - Details of any training received (external LCFS only)
    - Date of nomination form (external LCFS and DOF only)
    - Details of nomination i.e. List of nominated orgs past and present, with details of whether Lead or Support LCFS
    - Security Questions
    - Individual user ID and passwords for access to NHS Protect systems.

2. The impact level of the CPOD information was assessed at OFFICIAL and the information is only accessed internally.

3. The following measures briefly describe what controls have been implemented to protect CPOD and the personal data recorded in the application:

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

    b. CPOD is only available to internal NHS Protect staff and is not accessible externally

    c. CPOD is available to all staff members with restrictions where appropriate depending on the level of access required in their role.

    d. There is a direct interfaces / interconnections with iBase (another NHS Protect application) as part of an automatic process.

    e. There is functionality within the application to export data via excel, pdf or csv files.

    f. The CPOD 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 NHSP register and the NHS Protect DPO is aware of its existence.

    g. The login passwords for CPOD do not expire and as such the password would only be reset if the user requested it.

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

Introduction

5. CPOD is an application designed and developed by NHS Protect. Internal and external contacts are recorded and recognised by their unique identification number which is generated by the system when a new user is created. The application is used as a consistent central directory for internal staff to search and view contact information. It is also used to facilitate the nomination process/ new user requests for Local Counter Fraud Specialists and Directors of Finance and holding individual passwords and answers to security question, is the only mechanism by which these external contacts would be granted access to other NHS Protect applications and systems.

Section 1: Data Collection and Maintenance

6. Personal data collected by the application is mainly Business Card Information and includes name, date of birth, NHS employment information, contact telephone number, email address and details of any training and nominations to organisations. However there

7. This PIA must be reviewed if any changes are made to the personal information if used by the CPOD application or any other changes are made that affect the privacy of an individual.

8. The privacy risks and associated mitigations are described in Table 4. The IAO is responsible for mitigating the risk and their responsibilities are defined in the CPOD 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.	All personal data received by NHS Protect is encrypted upon receipt. Access to this data is only possible via the Database Administrators, via a login and password Users are only given sufficient rights to systems to enable them to perform their specific job function. User rights will be kept to the minimum required to do their job effectively and efficiently. Access rights are reviewed on a monthly basis.
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. The data collected in this application is mainly Business Card Information of which the data subjects are aware.
3. There is a risk that personal data is retained for longer than necessary.	CPOD is subject to NHS Protect Data Handling and Storage Policy currently in draft as of 28/07/17)) 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.	As the data is mainly Business Card Information and does not contain sensitive information, the only aspect that would no longer be relevant would be the NHS employer. However as CPOD has a direct impact on the nomination process and access to NHSProtect systems, any changes would be updated accordingly.

Risk Description	Mitigation
5. There is a risk that the personal data is not accurate or up to date.	CPOD data is provided by the individual themselves by way of a nomination form or from personal records for internal staff. The responsibility for accuracy lies with the external person completing the nomination form or internal staff transferring the information to the system.
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 CPOD Risk Assessment Report 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. The only information that would be shared would be the names of any nominated /accredited persons Local Counter Fraud Specialists (LCFS) and Directors of Finance (DOF) within their own organisation.
8. There is a risk that personal data is hosted or exported outside of the EU.	CPOD will only be hosted in the UK and no data will be exported outside the UK

Table 4 – Privacy Risks

Section 2: Uses of the Application and the Data

9. CPOD holds details of internal staff and is also predominant to the nomination process for external Local Counter Fraud Specialists and Directors of Finance, and Audit Committee Chair. The system also holds records of NHS organisations which are imported on a monthly basis as part of an automatic process.

10. The information is collected for the purpose of having consistent contact information in one application as well as facilitating a process to enable access to other NHSProtect systems and applications.

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

a. Access to CPOD can only be gained by Internal NHS Protect staff, and there is currently an expectation of no more than 200 users of the application.

b. All Users account creation, passwords and access have to be authorised by the NHS Protect Service Desk.

c. CPOD passwords do not expire and would only be reset if the user requested it.

d. There is a direct interface/interconnection with iBase (another NHS Protect application) as part of an automated process.

e. There is no functionality within the application to export data via excel, pdf or csv files.

f. The CPOD Data Custodian must comply with the 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

12. Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. The maximum period depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found 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 as described in the FIRST SyOPs and if there is a requirement to change the retention period the change must be submitted to the Application Change Board,.

13. The current retention schedule as detailed above has been approved by the Data Protection Officer.

Section 4: Internal Sharing and Disclosure of Data

14. CPOD is only used internally by NHS Protect staff who have been allocated different permission levels depending on their role.

Section 5: External Sharing and Disclosure of Data

15. No personally identifiable information would be shared with external organisations as it would contravene data protection. However the information held within CPOD would mainly be Business Card Information including name, post/role, work email and telephone number which is not classed as personal information.

Section 6: Notice/Signage

1. CPOD is essentially a contact directory of Business Card Information of which the data subjects are aware. This is particularly significant for External contacts would not be granted access to our systems should we not have this information.
2. 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.
3. The use of signage or other notifications to notify the public of the gathering and use of personal is not relevant to this dataset, and therefore outside the scope of this PIA.

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

16. 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.

17. It is unlikely that many access requests will be received, as the information held in CPOD is mainly classed as Business Card Information which has been provided to us by the individual themselves.

18. In the unlikely event that that information in relation to the subject is identified as being incorrect the CPOD administrators would correct the record.

19. 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

20. The security and technical access architecture of the CPOD application is described in the CPOD Risk Assessment Report. The application and the hosting infrastructure was assessed at Official. The application is subject to CESG approved IT Security Health Checks

21. As CPOD is restricted to internal NHS Protect staff only, there is expected to be no more than approximately 200 users of the application. Staff have been allocated different permissions within the system dependant on their job role and whether they need read only or the ability to input information. As the total number of User accounts is less than 1000, they are manually managed by NHS Protect Database Administrators.

22. The technical controls to protect the application and the CPOD information include:

a. Anti-virus protection for the underlying infrastructure;

b. Role based access controls;

c. Password complexity;

d. Patching Policy for the underlying infrastructure;

e. Encryption;

Section 9: Technology

23. CPOD is the Central Person and Organisation Database. Within the database reside records detailing individuals who either work for NHS Protect (internal staff) or individuals who require access to our systems and services (external staff). The database is located within the NHS Protect internal Oracle database infrastructure within the NHS Protect data centre. Records are maintained using the CPOD Admin Tool - a Java web application developed in house using the Java development language and a number of standard frameworks.

Conclusion

24. There are no residual privacy risks to the personal data recorded in CPOD. The controls described in this PIA and Risk Assessment Report describes 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 5: Compliance Checks

DPA 98 Compliance Check

1. The DPO must ensure that CPOD, 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 processes 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 – CPOD Personal Data

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

Ser	Personal Data	Justification
1	Unique user ID	Generated automatically when new person added to the system.
2	Name of Subject	Required to search for contact details, or nomination status in order to grant access to other systems.
3	Date of Birth of Subject	Collected only when provided as part of the initial nomination process.
4	Business address	This is regarded as Business Card Information
5	Home address	We would not request this and as such any personal addresses are provided voluntarily.
6	Contact details of Subject	Required as one of the main purposes of this contact directory of information.
7	Employment Details	Required to verify nomination status and grant access to other NHSCFA systems. Details of nominated organisations are linked to profiles.
8	Training Dates	Added as part of the nomination process to establish and ensure that the user has gained accreditation prior to nomination.
9	Individual Passwords to systems	Generated by NHS Protect and necessary to provide access to systems.
10	Security Questions	Security question responses are required to grant access to NHSProtect systems.

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	Central Person and Organisation Database (CPOD)

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, 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 Central Person and Organisation Database (CPOD) is an application that was developed to centralise the person and organisation data held by NHS Protect in one single source and to which other NHSProtect applications could refer. The system was created as a solution to the previous manual process which involved maintaining contact information in a number of different systems.

CPOD which has been in continuous development since its introduction in 2013, holds mainly Business Card information of internal and external contacts, details of NHS organisations, and is also predominant to the nomination process for external Local Counter Fraud Specialists and Directors of Finance.

CPOD is used internally by NHSProtect staff as a contact directory and dependent on user permissions, staff can create new contacts, search for persons and organisations and also export contact lists to excel, PDF or CSV files.

This PIA is developed by the Information Analytics Lead, in consultation with NHSProtect staff from a number or teams.

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. In particular, it has national responsibility for tackling fraud, as this has been identified a key activity that would otherwise undermine the effectiveness of the health service and its ability to meet the needs of patients and professionals.

To achieve this, NHS Protect collects data appropriate for preventing and detecting fraud within the NHS, remaining mindful that, where this includes personal data, the personal data is adequate, relevant and not excessive for the purposes for which it is processed.

In relation to the NHS BSA remit, Part 2, Section 12 of the NHS Business Services Authority Directions 2013 NHS Business Services Authority Directions4 2013 notes that the Authority must exercise (through NHS Protect) the functions in relation to counter fraud and security management specific in Schedule 1, which concerns itself with the functions of the authority in relation to counter fraud and security management.

Specifically, Section 9 of Schedule 1 notes the following function: "(to) obtain, monitor, collate and analyse such data as NHS Protect considers appropriate for the purposes of identifying trends and anomalies which may be indicative of fraud, corruption or other unlawful activities against or affecting the health service."

CPOD is the central contact directory holding the contact details of internal staff as well as those of external Local Counter Fraud Specialists(LCFS) and Directors of Finance (DOF) which is necessary for the engagement and facilitation in fraud prevention.

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

Privacy impacts have been considered in the light of personal data gathered, however the data collected in this application is mainly Business Card Information of which the data subjects are aware.

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

Full PIA completed in May 2017

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)

[4] http://www.nhsbsa.nhs.uk/Documents/Sect_1_-_B1_BSA_Directions_2013.pdf

PART 2 – DATA PROTECTION PRINCIPLES

DPA PRINCIPLE	SUB-SECTION	QUESTION	Y/N	RESPONSE
No.1 – Fair and Lawful Processing	**1.1 Preliminary** **Personal data shall be processed fairly and lawfully**	1. What type of personal data are you processing? Please give examples of any sensitive personal data that you are processing.	Y	Unique user ID Name of Subject Date of Birth of Subject Business Address of Subject Personal Address of Subject Contact details: email and telephone numbers NHS Employment / links to NHS for Subject Training Dates of Subject Individual Passwords Responses to security questions.
		2. Are sensitive personal data being differentiated from other forms of personal data? If yes, please specify procedures. If no, please indicate why not.	Y	NHS Protect protects information in a manner appropriate to its sensitivity, value, and criticality The data in CPOD is mainly Business Card Information, however this and any limited personal information that might be collected would not be shared externally.
	1.2 Schedule 2 - Conditions relevant for purposes of the first principle: processing of any personal data	1. Have you identified all the categories of personal data that you will be processing and how? If yes, please list them. If no, please indicate why not.	Y	Details of the Data Subject

		2. Have you identified the purposes for which you will be processing personal data and how? If yes, please list them. If no, please indicate why not.	Y	The data is required for the following purposes: To create a contact directory to search and locate details of individuals. To facilitate a process to provide access to NHS Protect systems and applications.
		3. Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data? If yes, please list them. If no, please indicate why not.	Y	The processing is necessary under Schedule 2 For the administration of justice. • To provide access to NHS Protect systems and applications
		4. Are you relying on different grounds for different categories of personal data? If yes, how will this assessment be made?	N	N/A – it is generally all processed under the same grounds noted in Annex B

	1.3 Schedule 3 - Conditions relevant for purposes of the first principle: processing of sensitive personal data If this project does not involve the processing of sensitive personal data, please go to section 1.4	1. Have you identified the categories of sensitive personal data that you will be processing? If yes, can you list them? If no, please indicate why not.	N/A	
		2. Have you identified the purposes for which you will be processing sensitive personal data? If yes, can you list them? If no, please indicate why not.	N/A	
		3. Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data? If yes, can you list them? If no, please indicate why not.	N/A	
		4. Are you relying on different grounds for different categories of sensitive personal data? If so, how will this assessment be made?	N/A	

	1.4 Obtaining consent	1. Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2? If yes, when and how will that consent obtained?	N	Individuals are aware of the information held for them as follows: for internal staff, the individual can view the information and for external subjects, they have provided us with the information in order to arrange access to NHS Protect systems and applications.
		2. For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act? If so, when and how will that consent obtained?	N/A	There is no sensitive personal data collected in the application.
	1.5 Lawful processing	1. If you are a public sector organisation, does your processing of personal data fall within your statutory powers? If yes, please state what they will be. If no, please indicate why not.	Y	The processing is formalised via the Secretary of State directions to “obtain, monitor, collate and analyse such data held by any NHS body or local authority as the NHS Protect consider appropriate for the purposes of identifying trends and anomalies which may be indicative of fraud, corruption or other unlawful activities against or affecting the health service.” (As detailed in the NHS Business Services Authority Directions 2013 , schedule 1 part 9
		2. How is compliance with the Human Rights Act being assessed?	Y	The Information held within CPOD has been audited to ensure compliance with the Human Rights Act

		3. Are you assessing whether any of the personal data being processed is held under a duty of confidentiality? If yes, how will that assessment made? If no, please indicate why not.	Y	NHS Protect is fully compliant with the HMG Information Assurance Standard IS1 and IS2 standards. The assessment of duty of confidentiality forms part of a Risk assessment conducted in accordance with these standards.
		4. How is that confidentiality maintained? (e.g. instructions on disclosure or shredding)	Y	NHS Protect Information Security Policy and Acceptable Use Policy covers all elements of appropriate behaviour with confidential information. NHS Protect staff are expected to follow these requirements and are subject to annual refresher training (with a subsequent examination)
		5. Are you assessing whether your processing is subject to any other legal or regulatory duties? If yes, how is that assessment being made? If no, please indicate why not.	Y	NHS Protect has an Information Governance and Risk Management Lead who is able to stay cognisant of legal issues and changes to the legalities of data user Yes. As part of this DPA Compliance Check and the related PIA this has been reviewed. Additionally, NHS Protect submits an annual IG Toolkit, in relation to the data captured and processed by the organisation, to demonstrate the NHS BSA policies and procedures it is managed in accordance with.

		6. How are you ensuring that those legal duties are being complied with?	Y	NHS Protect is audited annually against the ISO 27001 information standard (formally known as ISO/IEC 27001:2005) this is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
	1.6 Fair processing	1. Are individuals being made aware of the identity of your organisation as the data controller? If yes, state how they are being made aware. If no, please indicate why not.	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. Individuals are aware of the data we hold for them as they either have access to the information themselves or have provided us with the information to be granted access to NHS Protect applications and systems.
		2. How are individuals being made aware of how their personal data is being used?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. Individuals are aware of the data we hold for them as they either have access to the information themselves or have provided us with the information to be granted access to NHS Protect applications and systems.

		3. How are individuals offered the opportunity to restrict processing for other purposes?	Y	This information is not processed for any other purposes.
		4. Do you receive information about individuals from third parties? If yes, please give examples. If no, please go to section 1.7	N	NB ..Only if the nominations form containing the individual's details, is received indirectly from someone else within their organisation.
		5. How are individuals informed that the data controller is holding personal data about them?	Y	Although Individuals usually know what we hold in CPOD, they may still enquire by way of a request, if the organisation holds personal information about them. Details are available on the BSA website on how to make this request.

	1.7 Exemptions from the first data protection principle The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller 2. the identify of any nominated data protection representative, where one has been appointed 3. the purpose(s) for which the data are intended to be processed 4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair Data Protection Act, Schedule 1, Part II, para. 2 (3)	1. Do you provide individuals with all of the information described in 1.7? If no, which exemption to these provisions is being relied upon?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. Data in relation to the individual is limited and has been provided by them voluntarily.

No.2 - THE PURPOSE OR PURPOSES FOR PROCESSING PERSONAL DATA Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	**2.1 Use of personal data within the organisation**	1. Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?	Y	Information Asset register and annual risk assessment.
		2. How often is this record checked?	Y	Every two months (prior to update of IT Security Forum.
		3. Does the record cover processing carried out on your behalf (e.g. by a subcontractor)?	Y	N/A - No processing is carried out on behalf of NHS Protect
		4. What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data? (Cross reference with section 1.6, Fair Processing)	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. Individuals are aware of the data we hold for them as they either have access to the information themselves or have provided us with the information to be granted access to NHS Protect applications and systems.

	2.2 Use of existing personal data for new purposes	1. Does the project involve the use of existing personal data for new purposes? If no, go to section 2.3	N	N/A
		2. How is the use of existing personal data for new purposes being communicated to:- (a) the data subject; (b) the person responsible for Notification within the organisation (c) the Information Commissioner?		N/A
		3. What checks are being made to ensure that further processing is not incompatible with its original purpose?		N/A
	2.3 Disclosure of data	1. Do you have a policy on disclosure of personal data within your organisation / to third parties? Is it documented?	Y	Contained within the Information Security Policy and Acceptable Use Policy

		2. How are staff made aware of this policy / instructed to make disclosures?	Y	Available on NHS Protect Intranet. Additionally, staff are expected to complete refresher training on a yearly basis (with subsequent examination) in relation to these principles.
		3. How are individuals / data subjects made aware of disclosures of their personal data?	Y	ICO Notification of Data Controllers list all the information described in 1.7. This information is available via the ICO website and additionally on the NHS Protect website. Individuals are aware of the data we hold for them as they either have access to the information themselves or have provided us with the information to be granted access to NHS Protect applications and systems.
		4. Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed? If no, go to section 3.1 If yes, how do you make the assessment?	Y	Requests must be made in writing, explaining the use of personal data being disclosed and information will only be disclosed once authorised by NHS Protect Data protection Officer. They would also be subject to the process for requesting personal data via written authorisation
No. 3 - ADEQUACY AND RELEVANCY	**3.1 Adequacy and relevance of personal data**	1. How is the adequacy of personal data for each purpose determined? (Please give examples.)	Y	The same personal data is collected for everyone as defined by selection categories in the database. Additional data may be held for external individuals but they would be aware of it as they have provided the information voluntarily.

		2. How is an assessment made as to the relevance (i.e. no more than the minimum required) of personal data for the purpose for which it is collected? Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this system.
		3. What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this project.
		4. How often will these procedures reviewed?	Y	At any point at which the contents of the above document are deemed either out of date or no longer relevant due to changes to the data capture and outputs.
		5. Are there procedures for assessing the amount and type of personal data collected for a particular purpose? If yes, please describe. If no, please indicate why not.	Y	This forms an integral part of the Privacy Impact Assessment that has been completed for this project.
		6. Are items of personal data held in every case which are only relevant to a subset of those cases?	N	N/A

No. 4 - ACCURATE AND UP TO DATE Personal data shall be accurate and, where necessary, kept up to date.	**4.1 Accuracy of personal data**	1. How, and how often, are personal data checked for accuracy? Please give examples:	Y	Information is provided by external individuals themselves or from personal records for internal staff. We know that Business Card Information is correct as it is backed up by a nomination form or from personnel records. However for any other information it would only be as accurate and up to date as the data with which we have been provided
		2. Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?	Y	This is not relevant, as the system holds mainly Business Card information which has been provided by the subjects themselves. As such, there should be no inaccuracy.
		3. In what circumstances is the accuracy of the personal data being checked with the Data Subject? Please give examples:	Y	On receipt of a nomination form.
		4. Are the sources of personal data (i.e. data subject, data controller, or third party) identified in the record? If so, how? Please give examples:	Y	The source of the personal data would be the individual themselves or a third party from the same organisation. Due to the nature of the data and the application itself, the source of the personal data would always be known.

		5. Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate? If no, please indicate why not.	Y	All request by the data subject are recorded by NHSP Data Protection Officer
	4.2 Keeping personal data up to date	1. Are there procedures to determine when and how often personal data requires updating?	N	There is no process possible by NHS Protect to determine when information should be updated, as there is no means to audit or review for accuracy – information is assumed accurate as provided (but caution is applied for use as a result) We would update either if we received new information or we were requested to do so.
		2. Are personal data evaluated to establish the degree of damage to: (a) the data subject or (b) the data controller that could be caused through being out of date? Please specify whether to data subject or data controller:	Y	This is not relevant, as the system holds mainly Business Card information which has been provided by the subjects themselves. As such, there should be no inaccuracy.

		3. Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?	Y	There is no process possible by NHS Protect to determine when information should be updated, as there is no means to audit or review for accuracy – information is assumed accurate as provided ..We would update either if we received new information or we were requested to do so. However, as the system holds mainly Business Card information which has been provided by the subjects themselves. there should be no inaccuracy.
No. 5 - NO LONGER THAN NECESSARY	**5.1 Retention policy**	1. What are the criteria for determining retention periods of personal data? How often are these criteria reviewed?	Y	This is documented in the NHS Protect Data Handling and Storage Policy currently in draft as of 28/07/17))
		2. Does the project(s) include the facility to set retention periods?	Y	This is a feature included in the process
		3. Is the project subject to any statutory / organisational requirements on retention? If yes, please state relevant requirements:	Y	Data will be retained only as long as necessary, up to a maximum period in accordance with the Data Protection Act 1998. The maximum period depends on whether fraudulent behaviour is detected – if fraud is found then the retention period is 7 Years, if fraud not found 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.

	5.2 Review and deletion of personal data	1. Is there a review policy and is it documented?	Y	This is documented in the NHS Protect Data Handling and Storage Policy currently in draft as of 28/07/17)
		2. When data is no longer necessary for the purposes for which it was collected: (a) How is a review made to determine whether the data should be deleted? (b) How often is the review conducted? (c) Who is responsible for determining the review? (d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	Y	Although there is a deletion process in place for the data held by NHS Protect, based on the age of the record. The process isn't applicable to this system as it is holds mainly Business Card Information and not personal information. This is audited annually as part of the impact assessment. The system doesn't have an automatic facility to identify records due for removal and as such this is a manual process. However as the records in CPOD relate to individuals who require access to our applications and systems and are determined by their unique user ID there is the possibility of there being historic Business Card Information for the purpose of reference and continuity of this access.
		4. Are there any exceptional circumstances for retaining certain data for longer than the normal period? If yes, please give justification:	N	No

		5. Is there any guidance on deletion / destruction of personal data? If no, please indicate why not.	Y	This is documented in the NHS Protect Data Handling and Storage Policy currently in draft as of 28/07/17)
No. 6 - SUBJECT ACCESS	**6.1 Subject access**	1. Are procedures in place to provide access to records under this Principle? If yes, please specify proposed procedures. If no, please indicate why not.	Y	There are processes in place for making a subject access request via the usual NHS BSA processes. The process for accessing the data for a subject access request would be the same for any other request (i.e. requiring written request, detailing the scope and extent of the personal info required and approval from the SRO prior to access to said data)
		2. How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?	Y	The personal data in CPOD is accessible by the unique user ID
		3. Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject? If yes, how? If no, please indicate why not	Y	Yes any codes and other information are explained to the data subject as part of the subject access request
		4. Are procedures in place to manage personal data relating to third parties? If yes, please specify proposed procedures. If no, please indicate why not?	Y	Limited Personal information relating to individuals is contained within CPOD, however there is no information held in relation to third parties.

		5. How is data relating to third parties managed?	Y	See Above
	6.2 Withholding of personal data in response to a subject access request	1. Are there any circumstances where you would withhold personal data from a subject access request? If no, go to section 6.3. If yes, on what grounds?	Y	Where exemptions allowable under section 7 of the DPA
		2. How are the grounds for doing so identified?	Y	Where this data is subject to inclusion in the detection of Fraud or as part of a fraud investigation (However it is unlikely that this would apply to CPOD)
	6.3 Processing that may cause damage or distress	1. Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual? If yes, please specify proposed procedures. If no, please indicate why not.		This is not relevant, as the system holds mainly Business Card information which has been provided by the subjects themselves. As such, there should be no inaccuracies to cause damage or distress to an individual.
		2. Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	Y	N/A
	6.4 Right to object	1. Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	N/A	N/A

	6.5 Automated decision-taking	1. Are any decisions affecting individuals made solely on processing by automatic means? If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	N	No - There is no automatic decision making in the CPOD System
	6.6 Rectification, blocking, erasure and destruction	1. What is the procedure for responding to a data subject's notice (in respect of accessible records) or a court order requiring: (a) rectification; (b) blocking; (c) erasure or; (d) destruction of personal data?	Y	It is the responsibility of the Data Protection Officer to respond to any notices or court orders; however it would be feasible to locate records for this purpose if required. It is possible that it may be necessary to block any requests from the data subject on the grounds of section 7 of the DPA
No.7 - SECURITY OF PERSONAL DATA	**7.1 Security Policy**	1. Is there a Data Security Policy? If no, please indicate why not and then go to 7.1, question 5.	Y	

		2. If yes, who / which departments are responsible for drafting and enforcing the Data Security Policy within the organisation?	Y	NHS Protects Information Systems and Security Dept.
		3. Does the Data Security Policy specifically address data protection issues?	Y	
		4. What are the procedures for monitoring compliance with the Data Security Policy within the organisation?	Y	Regular Audit by CESG and the BSI for continued ISO 27001 certification.
		5. Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?	Y	
		6. Is the level of security appropriate for the type of personal data processed?	Y	
		7. How does the level of security compare to industry standards, if any?	Y	Meets CESG requirements

	7.2 Unauthorised or unlawful processing of data	1. Describe security measures that are in place to prevent any unauthorised or unlawful processing of: (a) Data held in an automated format (e.g. password controlled access to PCs). (b) Data held in a manual record (e.g. locked filing cabinets)?	Y	Access to CPOD requires a password to access the system CPOD is only accessible to internal staff who are granted different levels of permission depending on their role. All off site back-ups are secure as they can only be opened via the encryption key. All CPOD personal data is stored electronic – no personal data should be in paper format beyond any immediate usage and disposal (should it prove necessary, the NHS BSA data confidentiality requirements for storing this data would apply).
		2. Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing? If yes, please describe the planned procedures. If no, please indicate why not.	N	There is no sensitive personal information in CPOD. However all off site back-ups are secure for data held by NHS Protect, as they can only be opened via the encryption key. NHS Protect protects information in a manner appropriate to its sensitivity, value, and criticality. As the combination of the entire dataset is a contribution to counter fraud investigations, the same robust security measures are therefore used regardless of the media on which information is stored within it. The systems which process it or the methods by which it is moved.

		3. Describe the procedures in place to detect breaches of security (remote, physical or logical)?	Y	Electronic: Next Generation approved firewalls and intrusion detection systems are installed. In addition to this NHS Protect have a log monitoring system in place to provide proactive SIEM monitoring. Physical: Swipe card access to the Data centre containing the SIRS system CCTV with 24/7 recording in the Data centre Remote & logical Protected by Firewalls and Intruder detection systems All security incidents logged with the Information Security Manager and Information Security Officer
	7.3 Destruction of personal data	1. Describe the procedures in place to ensure the destruction of personal data no longer necessary?	Y	It is the responsibility of the data protection officer to ensure destruction of personal data that is no longer necessary. 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
		2. Are there different procedures for destroying sensitive personal data?	N	N/A

	7.5 Contingency planning - accidental loss, destruction, damage to personal data	1. Is there a contingency plan to manage the effect(s) of an unforeseen event?	Y	Business Continuity and Disaster Recovery plans are fully documented and up to date
		2. Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through: • human error • computer virus • network failure • theft • fire • flood • other disaster.	Y	A full Business Continuity Plan (BCP) is in place and disaster recovery was successfully tested in November 2016. For further details see NHS Protect BCP, available from NHS Protect intranet.
	7.6 Choosing a data processor	1. What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?	N/A	The information is only processed by NHS Protect
		2. How did you assess their data security measures?	N/A	The information is only processed by NHS Protect
		3. How do you ensure that the Data Processor complies with these measures?	N/A	The information is only processed by NHS Protect

		4. Is there an on-going procedure for monitoring their data security measures? If yes, please describe. If no, please indicate why not.	N/A	The information is only processed by NHS Protect
No. 8 - OVERSEAS TRANSFER The European Economic Area (EEA) comprises the 27 EU member states plus Iceland, Liechtenstein and Norway. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	**8.1 Adequate levels of protection**	1. Are you transferring personal data to a country or territory outside of the EEA1? If no, please go to Part 3.	N	There is no transfer outside the EEA

		2. What are the types of data are transferred? (e.g. contact details, employee records)	N/A	
		3. Are sensitive personal data transferred abroad? If yes, please provide details:	N	
		4. What are the main risks involved in the transfer of personal data to countries outside the EEA?	N/A	There is no transfer outside the EEA
		5. Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	N/A	There is no transfer outside the EEA
		6. Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	N/A	There is no transfer outside the EEA
	8.2 Exempt transfers	1. Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply? If yes, what are they?	N	There is no transfer outside the EEA
		2. To which country / territory are these transfers made?	N/A	There is no transfer outside the EEA

		3. What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle? E.g. consent, (See DPA 1998, Schedule 4, for a full list)	N/A	There is no transfer outside the EEA

PART 3 – DATA PROTECTION PRINCIPLES (DPP) COMPLIANCE – CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

CPOD complies with the requirements of the Data Protection Act (DPA98).

_____ _____
(Proponent) (Data Protection Officer)

Date: _____ Date: _____